PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS Y COMPUTACION

DESARROLLO DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS CON UN CONTROLADOR DE DOMINIO PRINCIPAL EN UN ENTORNO DE ALTA DISPONIBILIDAD SOBRE UNA PLATAFORMA LINUX.

JORGE LUIS ARMIJO QUITO

DIRECTORA: ING. BEATRIZ CAMPOS

QUITO, 2014

DEDICATORIA

Con todo mi cariño y mi amor para mis papis que hicieron todo para que pueda cumplir con mis sueños y mis metas.

Gracias Mamita por su inmenso sacrificio sin el cual no hubiese podido culminar con esta etapa muy importante en mi vida.

Muchas gracias Papito por tus consejos y por siempre estar junto a mí apoyándome cuando el camino se volvía difícil.

Gracias padres míos desde lo más profundo de mi corazón por siempre brindarme su apoyo este trabajo se los dedico enteramente a ustedes.

Martha y Jorge

DEDICATORIA

A mis viejitos adorados mis abuelitos que siempre estuvieron a mi lado desde cuando era muy pequeño hasta el día de hoy que me han visto ya convertido en un hombre, gracias viejitos que sin ustedes este sueño no lo hubiese podido culminar. En especial a ti abuelita que siempre has estado al pendiente de mi por cuidarme, mimarme e inculcarme el respeto y el amor por los demás. A ti mi Abuelito mil gracias por enseñarme que la verdadera felicidad en la vida se consigue haciendo lo que realmente uno ama hacer.

Beatriz y Jorge

DEDICATORIA

A ti mi amada Andreita por tu paciencia, comprensión y apoyo incondicional para que yo pudiera cumplir con mis sueños y mis metas. Con tu bondad y sacrificio me inspiraste para nunca decaer y seguir adelante a pesar del cansancio. Esta Tesis lleva mucho de ti gracias por estar siempre a mi lado siempre demostrando tu apoyo. Te Amo.

Andreita

AGRADECIMIENTOS.

Gracias a mis maestros por abrirme las puertas a una experiencia universitaria llena de alegrías vivencias y retos, mil gracias por entregar lo mejor de sus conocimientos, consejos, experiencias y sabiduría que sin duda influyeron en mí para formarme como una persona de bien y preparada para los retos que la vida me impone día a día, a cada uno de ustedes les dedico este trabajo.

Ing. Beatriz Campos
Ing. Susana Masapanta
Ing. Xavier Cóndor

AGRADECIMIENTOS.

Como poder dejar de lado y dar las gracias a las personas que gracias a ellos y la visión que tuvieron hace ya 9 años llegaron a formar Soporte Libre empresa en la cual me he llegado a sentir como en mi segundo hogar y en la cual he podido realizarme como un profesional, cumpliendo así con uno de mis sueños haciendo lo que realmente me hace feliz, gracias por la confianza que me brindaron, por dejarme demostrar mis habilidades y en mi empeño por realizarlas, por permitirme cumplir con mis objetivos y mis sueños y sobre todo por brindarme todo su apoyo incondicional no solo como jefes sino como amigos, ahora me toca regresar un poquito de lo inmenso que me han otorgado con todo mi cariño esta tesis se las dedico.

Leslie y Ricardo

TABLA DE CONTENIDOS.

1. INTRODUCCIÓN A LOS SERVIDORES DE DOMINO. 1

1.1. ¿QUÉ ES UN SERVIDOR DE DOMINO? 1
1.2. ANÁLISIS DE LOS PRINCIPALES SERVIDORES DE DOMINIO. 2
1.2.1. SERVIDORES DE DOMINIO PRIVATIVOS. 2
1.2.1.1. Servidor de Dominio NT. 2
1.2.1.2. Servidor de Dominio NT 3.0. 2
1.2.1.3. Servidor de Dominio NT 4.0. 2
1.2.1.4. Servidor de Dominio Windows Server 2000. 3
1.2.1.5. Servidor de Dominio Windows Server 2003. 3
1.2.1.6. Servidor de Dominio Windows Server 2008. 4
1.2.2. SERVIDORES DE DOMINIO OPEN SOURCE. 4
1.2.2.1. Novell Directory Services. 4
1.2.2.2. Sun ONE Directory Server. 4
1.2.2.3. Open Ldap. 5
1.2.2.4. Samba. 5
1.2.2.5. 389 Directory Server. 5
1.2.2.6. Red Hat Directory Server. 6
1.2.2.7. Apache Directory Server. 6
1.3. DIFERENCIAS ENTRE ACTIVE DIRECTORY Y DOMINIOS WINDOWS NT. 7
1.4. DIFERENCIAS ENTRE ACTIVE DIRECTORY Y UN LDAP. 7
1.5. DIFERENCIAS ENTRE UN DOMINO WINDOWS NT Y LDAP 8
1.6. PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS (LDAP). 8
1.7. VENTAJAS EN EL USO DE LDAP. 10
1.8. HISTORIA DEL LDAP Y ESTÁNDARES UTILIZADOS 10
1.9. LDAP ESTÁNDARES. 12
1.9.1. RFC 1274 THE COSINE AND INTERNET X.500 SCHEMA. 12
1.9.2. RFC 1777 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (V2). 12
1.9.3. RFC 2251 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (V3). 12
1.9.4. RFC 2252 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (V3): ATTRIBUTE SYNTAX DEFINITIONS. 13
1.9.5. RFC 2253 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (V3): UTF-8 STRING REPRESENTATION OF DISTINGUISHED NAMES 14
1.9.6. RFC 2254 THE STRING REPRESENTATION OF LDAP SEARCH FILTERS. 14
1.9.7. RFC 2255 THE LDAP URL FORMAT. 14
1.9.8. RFC 2256 A SUMMARY OF THE X.500 USER SCHEMA FOR USE WITH LDAPV3. 15
1.9.9. RFC 2829 AUTHENTICATION METHODS FOR LDAP. 15
1.9.11. RFC 2849: THE LDAP DATA INTERCHANGE FORMAT (LDIF) 15
1.10. DIFERENCIAS ENTRE UN LDAP Y UNA BASE DE DATOS. 16

1.11. Características de un LDAP. 16
1.11.1. Escalabilidad. 16
1.11.2. Disponibilidad. 17
1.11.3. Seguridad. 17
1.11.4. Gestionabilidad. 17
1.11.5. Estandarización. 18
1.11.6. Operaciones de lectura muy rápidas. 18
1.11.7. Datos relativamente estáticos. 18
1.11.8. Entorno distribuido. 18
1.11.9. Estructura jerárquica. 19
1.12. Arquitectura del LDAP. 19
1.12.1. Componente de Información. 19
1.12.2. Componente de Nomenclatura. 20
1.12.3. Componente Funcionalidad. 21
1.12.4. Componente de Seguridad. 22
1.13. Arquitectura Cliente – Servidor del servicio de Directorio. 22
1.14. Directorios Distribuidos. 23
1.15. Seguridad del directorio. 23
1.15.1. Autenticación Anónima. 23
1.15.2. Autenticación Básica. 23
1.15.3. SSL and TLS 24
1.15.4. SASL. 24
1.16. Información que se almacena en un LDAP. 25
1.16.1. Entradas. 25
1.16.2. Objetos. 26
1.16.3. Atributos. 26
1.16.4. Tipos de Atributos. 27
1.16.4.1. Atributos Obligatorios. 27
1.16.4.2. Atributos Opcionales. 27
1.16.5. Atributos de Objetos más usados. 27
1.16.6. Esquemas. 28
1.16.7. Tipos de Esquemas de un LDAP. 29
1.16.8. Archivos LDIF. 30
1.17. Estructura de la Información dentro del LDAP. 30
1.18. Indexación de la Información de un LDAP. 30
1.19. Filtros de búsqueda en LDAP. 31
1.20. Estándar sistemas x.500. 31
1.21. Diferencia entre versiones del LDAPv2 y LDAPv3. 33
1.22. Protocolos de Sincronización LDAP. 34
1.23. Tipos de Sincronización y Replicación. 34
1.23.1. Sincronización y Replicación con slurpd, slapd. 34

1.23.2. Sincronización y Replicación con SynRepl. ... 35
1.24. **Replicación.** ... **36**
1.24.1. Replicación Maestro – Esclavo. ... 38
1.24.2. Replicación Múltiples Maestros. ... 39
1.25. Autenticación y Autorización. ... **40**
1.26. Mantenimiento del directorio Activo. ... **41**
1.26.1. Mantenimiento de la Información. ... 41
1.26.1.1. Fuente de datos de origen. ... 41
1.26.1.2. Controles al azar. ... 42
1.26.1.3. Encuestas a usuarios. ... 42
1.26.2. Respaldo y sistema de recuperación de desastres. ... 42
1.27. Controlador de Dominio Primario. ... **43**
1.27.1. ¿Qué es un Controlador de Dominio? ... 43
1.27.2. ¿Qué es un Dominio NetBios? ... 44
1.27.3. ¿Qué es un grupo de Trabajo? ... 45
1.27.4. Samba y OpenLdap como controladores de Dominio. ... 45
1.28. Ventajas al uso de un Controlador de Dominio ... **47**
1.29. Tipos de Controladores de Dominio ... **48**
1.30. Administración de Usuarios y Grupos ... **49**
1.31. Servicios que implementa el uso del servidor PDC-SAMBA ... **49**
1.32. Alta Disponibilidad ... **52**
1.32.1. ¿Qué es la Alta Disponibilidad? ... 52
1.32.2. Factores que afectan la alta disponibilidad. ... 53
- *El software.* ... 53
- *Consideraciones del entorno físico sobre los equipos.* ... 54
- *Operaciones sobre la red y errores humanos.* ... 54
  - *Predicción.* ... 55
  - *Medición.* ... 55
  - *Análisis.* ... 55
  - *Gestión de Cambios.* ... 55
- *El mismo diseño de la red.* ... 55

1.32.3. ¿Qué es un único punto de fallo? ... 56
1.33. Ventajas de Usar alta disponibilidad. ... **56**
1.34. Recursos de un Sistema de Alta Disponibilidad. ... **57**
1.34.1. Nodos. ... 57
1.34.2. Sistemas de Almacenamiento. ... 57
1.34.3. Sistema Operativo. ... 57
1.34.4. Conexiones de red. ... 57
1.34.5. Middleware. ... 58
1.34.6. Aplicaciones. ... 58
1.35. Redundancia en un entorno de Alta Disponibilidad. ... **58**

1.35.1. REDUNDANCIA HARDWARE O FÍSICA. 58
1.35.2. REDUNDANCIA SOFTWARE. 59
1.35.3. REDUNDANCIA INFORMACIONAL. 59
1.35.4. REDUNDANCIA TEMPORAL. 59
1.36. SERVICIO DE DATOS EN UN ENTORNO DE ALTA DISPONIBILIDAD. 59
1.37. TIPOS DE ALTA DISPONIBILIDAD. 60
1.37.1. ALTA DISPONIBILIDAD A NIVEL DE HARDWARE. 60
1.37.2. ALTA DISPONIBILIDAD A NIVEL DE APLICACIÓN. 60
1.38. CONFIGURACIONES DE ALTA DISPONIBILIDAD. 60
1.38.1. CONFIGURACIÓN ACTIVO/ACTIVO. 60
1.38.2. CONFIGURACIÓN ACTIVO/PASIVO. 61
1.39. INTEGRIDAD DE DATOS Y RECUPERACIÓN DE SERVICIO 62
1.40. NIVELES DE DISPONIBILIDAD DEL SISTEMA. 67
1.41. GLOSARIOS DE TÉRMINOS. 68

2. DESARROLLO DE LA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS CON UN CONTROLADOR DE DOMINIO PRINCIPAL EN UN ENTORNO DE ALTA DISPONIBILIDAD. 70

2.1 INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO. 70
2.1.1 INSTALACIÓN DEL SISTEMA OPERATIVO. 71
2.1.1.1 Selección del medio de Instalación y versión del Sistema Operativo. 72
2.1.1.2 Asignación de memoria. 73
2.1.1.3 Asignación del espacio de almacenamiento. 73
2.1.1.4 Configuración de interface de red. 74
2.1.1.5 Instalación del Sistema Operativo. 75
2.1.1.6 Seleccionar Idioma para la instalación del Sistema Operativo. 77
2.1.1.7 Seleccionar el teclado apropiado. 77
2.1.1.8 Seleccionar el o los dispositivos de disco para realizar la instalación. 78
2.1.1.9 Configuración de hostname para el sistema virtualizado. 79
2.1.1.10 Configuración de la zona horaria. 79
2.1.1.11 Ingreso de la contraseña de root 80
2.1.1.12 Particionamiento del Sistema Operativo. 80
2.1.1.13 Configuración de contraseña para el grub. 82
2.1.1.14 Seleccionar el tipo de servidor que se instalara 82
2.1.2 CONFIGURACIÓN DEL SISTEMA OPERATIVO. 84
2.1.2.1 Configuración de la interface de red 84
2.1.2.2 Modificación para la resolución de nombres. 84
2.1.2.3 Configuración del repositorio de datos. 85
2.1.2.4 Configuración de almacenamiento compartido para OpenLdap. 86

2.1.2.5 Configuración de almacenamiento compartido para Samba. 89
2.2 INSTALACIÓN PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS LDAP. 92
2.2.1 INSTALACIÓN DEL OPENLDAP. 92
2.2.2 CONFIGURACIÓN OPENLDAP. 92
2.3 INSTALACIÓN DE UN CONTROLADOR DE DOMINIO PRIMARIO 97
2.3.1 INSTALACIÓN CONTROLADOR DE DOMINIO PRIMARIO. 97
2.3.2 CONFIGURACIONES CONTROLADOR DE DOMINIO PRIMARIO. 97
2.3.2.1 Global. 98
2.3.2.2 Netlogon. 100
2.3.2.3 Profiles. 100
2.4 ARCHIVOS DE CONFIGURACIÓN DE SAMBA Y LDAP. 100
2.4.1 INSTALACIÓN Y CONFIGURACIÓN DE LAS HERRAMIENTAS SMBLDAP-TOOLS 100
2.4.2 CONFIGURACIÓN DEL SMBLDAP.CONF 100
2.4.3 CONFIGURACIÓN DEL SMBLDAP_BIND.CONF 102
2.5 INGRESO DE INFORMACIÓN DEL ÁRBOL. 102
2.5.1 DEFINICIÓN DE LA ORGANIZACIÓN. 102
2.5.2 DEFINICIÓN DE LA ESTRUCTURA JERÁRQUICA DEL ÁRBOL. 102
***2.5.3* DEFINICIÓN DE CONJUNTO DE OBJETOS.** 103
2.5.4 DEFINICIÓN DE PERMISOS. 103
2.5.4.1 Usuarios Super Administradores. 104
2.5.4.2 Usuarios Administradores. 104
2.5.4.3 Usuarios Normales. 104
2.6 INSTALACIÓN Y CONFIGURACIÓN HERRAMIENTAS ADMINISTRACIÓN LDAP. 104
2.6.1 CONSIDERACIONES PREVIAS A LA INSTALACIÓN. 104
2.6.1.1 Versión del Sistema Operativo. 104
2.6.1.2 Versión OpenLdap. 104
2.6.1.3 Versión Samba 105
2.6.2 INSTALACIÓN PHPLDAPADMIN. 105
2.6.3 INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR WEB. 105
PARA LA INSTALACIÓN DE PHPLDAPADMIN EN UN TERMINAL EJECUTAR: 105
2.6.4 INSTALACIÓN Y CONFIGURACIÓN DEL PHPLDAPADMIN. 106
2.7 INSTALACIÓN DE UN SISTEMA DE ALTA DISPONIBILIDAD. 107
2.7.1 COMPATIBILIDAD DE VERSIONES SOFTWARE A INSTALAR. 107
2.7.2 INSTALACIÓN SISTEMA DE ALTA DISPONIBILIDAD. 107
2.7.3 INSTALACIÓN SISTEMA DE ALMACENAMIENTO COMPARTIDO. 107
2.7.4 INSTALACIÓN DE PAQUETES PARA LA ADMINISTRACIÓN DE FENCING. 107
2.7.5 CONFIGURACIÓN SISTEMA DE ALTA DISPONIBILIDAD. 107
2.7.5.1 Configuración del Administrador del Clúster. 107
2.7.5.2 Configuración de Nodos del Clúster. 108
2.7.6 CONFIGURACIÓN DEL SERVIDOR LDAP-SAMBA EN ALTA DISPONIBILIDAD. 108
2.7.6.1 Definición de las direcciones y hosts que intervendrán en el entorno de 108

Alta Disponibilidad. 108
2.7.6.2 Ingreso a la consola de administración de clúster. 108
2.7.6.3 Creación de un clúster. 109
2.7.6.4 Creación de un clúster 109
2.7.6.5 Definición de un dispositivo de fencing. 110
2.7.6.6 Definición de métodos de fencing para cada nodo del clúster. 111
2.7.6.7 Definición de un Dominio de cluster. 113
2.7.6.8 Definición de servicios del clúster. 114
2.7.6.9 Definición de grupos de servicios. 115
2.8 CONFIGURACIÓN DE SISTEMAS OPERATIVOS PARA LA INTEGRACIÓN CON EL LDAP-SAMBA. 116
2.8.1 CONFIGURACIÓN DE SISTEMAS OPERATIVOS DE CÓDIGO ABIERTO. 116
2.8.1.1 Configuración de red. 116
2.8.1.2 Configuración de credenciales de autenticidad. 117
2.8.2 CONFIGURACIÓN DE SISTEMAS OPERATIVOS LICENCIADOS. 119
2.8.2.1 Configuración de red. 119
2.8.2.2 Configuración Windows XP. 119
2.8.2.3 Configuración para Windows 7 y Windows 8 122

3. VALIDACIÓN DE LA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS CON UN CONTROLADOR DE DOMINIO PRINCIPAL EN UN ENTORNO DE ALTA DISPONIBILIDAD..... 129

3.1 INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO RHEL6.5..... 129
3.1.1 CONFIGURACIÓN HOSTNAME DEL EQUIPO. 130
3.1.2 CONFIGURACIÓN DEL REPOSITORIO LOCAL DE PAQUETES. 131
3.1.3 CONFIGURACIÓN DEL FIREWALL. 132
3.2 INSTALACIÓN PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS (LDAP). 133
3.3 INSTALACIÓN DE UN CONTROLADOR DE DOMINIO PRIMARIO. 134
3.4 CONFIGURACIÓN DE ARCHIVOS DEL LDAP. 136
3.4.1 CONFIGURACIÓN ARCHIVO PRINCIPAL PARA EL LDAP. 136
3.4.2 CONFIGURACIÓN DE CERTIFICADOS. 137
3.5 CONFIGURACIÓN DE ARCHIVOS DEL SAMBA. 137
3.5.1 CONFIGURACIÓN ARCHIVO PRINCIPAL PARA EL SAMBA 137
3.6 INGRESO DE INFORMACIÓN DEL ÁRBOL. 139
3.7 INSTALACIÓN Y CONFIGURACIÓN HERRAMIENTAS ADMINISTRACIÓN LDAP. 140
3.7.1 CONFIGURACIÓN SMBLDAP-TOOLS. 140
3.7.2 INSTALACIÓN Y CONFIGURACIÓN PHPLDAPADMIN. 142
3.8 INSTALACIÓN DE UN SISTEMA DE ALTA DISPONIBILIDAD. 142
3.8.1 INSTALACIÓN Y CONFIGURACIÓN DE LA CONSOLA DE ADMINISTRACIÓN 144
3.8.2 INSTALACIÓN Y CONFIGURACIÓN DE LOS NODOS DEL CLÚSTER. 145

4 CONCLUSIONES Y RECOMENDACIONES 148

4.1 CONCLUSIONES. 148
4.2 RECOMENDACIONES. 149

CAPITULO 1- MARCO TEÓRICO

1. INTRODUCCIÓN A LOS SERVIDORES DE DOMINO.

1.1. ¿Qué es un Servidor de Domino?[1] [2] [3]

Un servidor de dominio es un controlador de dominio el cual fue desarrollado por la Universidad de Michigan en la década de los 90, basado en los estándares X.500 de la ITU-T (International Telecommunication Union) que define un método estándar para acceder y actualizar información en un directorio. Se lo considera como una base de datos optimizada para el acceso a la lectura de información.

Este tipo de servidor lleva a cabo el proceso de administración de información de usuarios y equipos presentes en un sistema de red, su principal tarea es de proveer autenticación con los recursos de hardware y software en la red.

Un controlador de domino está basado en la administración de cuentas de seguridad SAM (Security Account Manager), el mismo que está conformado por archivos que contienen información de los usuarios y de sus credenciales de autenticación para su acceso a un domino de red, las cuales por motivos de seguridad se encuentran encriptadas, por lo tanto es mucho más eficiente tener la información centralizada antes que tenerla replicada cientos de veces en cada una de las estaciones de trabajo evitando con ello que la administración se torne difícil de controlar para los administradores de la red.

Un controlador de Dominio no es suficiente cuando los recursos en la red son numerosos por lo tanto es importante considerar la implementación de un servidor de dominio secundario en los sistemas de red, este tipo de servidor es conocido como BDC (Backup Domain Controller) que significa Controlador de Dominio Secundario el cual permite mantener un balanceo de carga sobre la administración de los recursos de la red, éste se encuentra sincronizado con un PDC (Primary Domain Controller) que significa Controlador de Dominio Primario, para mantener la integridad de la información del Dominio de Red.

---

[1] Daniel E. House, Tim Hahn. E-Directories Enterprise Software, Solutions, and Services, Addison-Wesley, Primera Edicion Julio 2000. Pág. 10

[2] Addison Wesley – Understanding and Deploying Ldap Directory Services 2Nd Ed 2003, Pág. 20

[3] Addison Wesley – Understanding and Deploying Ldap Directory Services 2Nd Ed 2003, Pág. 48

1.2. Análisis de los principales Servidores de Dominio.

1.2.1. Servidores de Dominio Privativos.

1.2.1.1. Servidor de Dominio NT.

Los servidores de dominio conocidos como NT "New Technology" iniciaron con las primeras computadoras de escritorio destinadas al uso en oficinas, en éstas específicamente es donde se presenta la necesidad de mantener un control y administración centralizado de las configuraciones del equipo, de esta manera se concibe la primera versión de un Controlador de Dominio Primario o Principal. Siendo esta una versión re-diseñada de la versión original creada por la Universidad de Michigan y sobre la cual Microsoft continuo desarrollando e implementando mejoras desde 1988, finalmente la primera versión estable comercial fue introducida en el mes de julio de 1993, obteniendo gran acogida en el mercado empresarial.

1.2.1.2. Servidor de Dominio NT 3.0.

Es la primera versión estable de un controlador de domino principal que público Microsoft publico junto con su versión de Sistema Operativo Windows Server NT en 1993. Esta versión de Microsoft Windows Server fue desarrollada por la demanda de fiabilidad que no presentaban anteriormente con su producto Windows 3.1. Es la primera versión de Windows dedicada a tareas de administración de Dominios, la cual presenta soporte para un solo Controlador de Domino Principal por red.

1.2.1.3. Servidor de Dominio NT 4.0.

Es una versión modificada de su antecesora con la diferencia que está basada sobre la interface de usuarios de Microsoft Windows 95 Workstation, su lanzamiento fue realizado en 1996, con esta versión Microsoft Windows y sus productos implementan en la rama de Servidores un cambio significativo sobre esta tecnología, siendo uno de estos el soporte para servidores de dominio secundarios dentro de un mismo segmento de red, facilitando a los administradores de la misma un manejo más prolijo de los recursos de hardware y software de acuerdo a las necesidades del mercado que se presentaba en esa época.

1.2.1.4. Servidor de Dominio Windows Server 2000.

Se encuentra sobre la última versión de Sistema Operativo Windows 2000, en la cual se incorporaron varias opciones especializadas para brindar servicios de Red con el objetivo de abarcar los Centros de Datos, ésta versión mostró avances sobre el manejo de sistemas Fat16, Fat32, NTFS, manejo para el cifrado de archivos, servicios de indexación, sistemas de respaldos, sistemas de tolerancia a fallos con discos dinámicos en la cual se incorpora la primera versión de Active Directory es decir se produjo un cambio completo en la estructura de la administración de los directorios NT que se manejaban, entre las principales características implementadas está el manejo de políticas de seguridad para los usuarios, como es la creación de perfiles y grupos de perfiles en los cuales se definen niveles de acceso, la mejora más considerables es la configuración de varios sistemas como Controladores Principales de Dominio.

1.2.1.5. Servidor de Dominio Windows Server 2003.

Tomando lo mejor de las Versiones de los Servidores NT en abril del 2003, Microsoft Windows Server 2003 es introducido en el mercado con características únicas hasta la fecha, entre las cuales simplifica la implementación, administración, y uso del sistema operativo, así también presenta notables mejoras en la interface de administración del servidor de dominio sobre la cual se implementa la funcionalidad de varios servidores principales y servidores de respaldo, como lo es el servidor de dominio, Active Directory, a partir de esta versión el servicio de NetBios es independiente separando la resolución de nombres al servidor de DNS que se incorpora en el Sistema Operativo.

Se implementa la principal herramienta de migración de la versión de controlador de dominio, lo cual permite migrar información de las estructuras de los árboles en las versiones de Windows NT 4.0, Windows 2000 a versiones de Active Directory de Windows Server 2003. Con la nueva versión de Active Directory y la flexibilidad que presenta ahora es posible la activación de nuevos atributos y definiciones de clases en el esquema que se encuentra definido en la instalación, permitiendo con ello la creación de grupos especializados de información.

1.2.1.6. Servidor de Dominio Windows Server 2008.

Active Directory en Windows Server 2008 corresponde a una actualización considerable del Active Directory de Windows Server 2003 en el cual se presentan modificaciones tanto en las herramientas de administración como en las interfaces de usuario. Entre las principales modificaciones presentes en esta versión de Active Directory están las mejoras en las herramientas de migración de Directorios Activos, con cambios en la Versión ADMT 2.0 permitiendo una fácil migración de claves de usuarios e integración con los nuevos esquemas implementados en la Nueva versión del Active Directory. A nivel de la Interfaz del Usuario se presenta una administración más sencilla de los componentes del Directorio, facilitando al usuario administrador el control de grupos creados en la estructura definida. Presenta también correcciones en los módulos de las políticas de seguridad, mejoras en el rendimiento y la confiabilidad de la información. Uno de los principales aportes de esta versión de Active Directory es que se basa en la definición de políticas de grupos GPO (*Group Policy* Object), lo cual permite la creación de secuencias de comandos, personalizar y automatizar la administración.

1.2.2. Servidores de Dominio Open Source.

1.2.2.1. Novell Directory Services.

Es una aplicación multi-plataforma que puede correr sobre cualquier sistema operativo (Linux, AIX, Solaris, Novell Netware, UNIX y además integra una versión de LDAP Nativo). Es considerado como servidor de dominio precursor en materia de estructuras de Directorio, ya que fue introducido en 1990 con la versión de Novell Netware4.0, a pesar de que Controlador de Dominio de Microsoft alcanzó mayor popularidad en esa época este no puedo igualar la fiabilidad que Novell Active Directory proporcionaba con su capacidad de ser implementado en múltiples plataformas.

1.2.2.2. Sun ONE Directory Server.

Es un componente de Java Enterprise System que anteriormente llevaba el nombre de iPlanet Directory Server basado en los protocolos x.500, es un tipo de LDAP (Lightweight Directory Access Protocol) que es un Protocolo Ligero de Acceso a Directorios diseñado para gestionar directorios de usuarios y recursos de la red, incluye su propia consola con la cual se lleva a

cabo las tareas de administración del directorio activo.

1.2.2.3. Open Ldap.

Es una versión libre de LDAP que como ya hemos mencionado es un protocolo a nivel de aplicación que soporta un servicio de directorio. Se basa en el estándar de servicio de directorio X.500 y en su protocolo DAP (Directory Access Protocol) que significa Protocolo de Acceso a Directorios, se diseñó para ser un protocolo simple y eficiente, de ahí su terminología de Lightweight que significa ligero. Open Ldap implementa un subconjunto de operaciones que permite definir ACL (Listas de control de acceso) para el acceso a los datos que almacena el Directorio Activo. OpenLdap permite transmitir los datos sobre una capa segura como OpenSSL. Así también facilita la replicación de datos entre varios servidores similares para descongestionar los servidores principales y mantener un esquema de administración descentralizada sin perder la integridad de la información que ésta almacena. OpenLdap maneja esquemas de replicación que pude soportar varios servidores principales que se mantendrán sincronizados entre sí y múltiples servidores secundarios que compartirán un tipo de sincronización asíncrona.

1.2.2.4. Samba.

Pese a que Samba por sí solo no es un Servidor de Dominio lo menciono en esta sección brevemente ya que en conjunto con los protocolos LDAP se consideran como un servidor de dominio, este servicio se ejecuta sobre plataformas Linux y emulan en conjunto con OpenLdap un Servidor de Domino Primario y un Directorio Activo comparándolos con la tecnología de Windows NT.

1.2.2.5. 389 Directory Server.

Es un servidor de dominio basado en LDAP que administra las configuraciones de perfiles de usuarios, información de grupos y políticas, así como también la información de control de acceso dentro de un sistema operativo independiente de la plataforma en la que sea alojada. Se encarga del manejo de la infraestructura de identidad. Provee una replicación multi-master permitiendo tener la misma información hasta en 4 servidores principales a la vez, presenta sincronización de usuarios grupos y contraseñas con Controladores de Domino de Windows

en sus versiones Windows NT 4.0, Server 2003 y Server 2008.

Permite la gestión de políticas de seguridad incluyendo las listas de control de acceso ACL (Access Control List) dentro de los atributos del objeto, facilita la implementación de las tareas de administración en un ambiente de producción sin tener que detener el servicio de directorio activo para tareas de respaldos, modificaciones de esquemas, modificación en políticas de seguridad.

1.2.2.6. Red Hat Directory Server.

Es un servidor que es compatible con el protocolo LDAP, basado en el proyecto 389 Directory Server se encarga de centralizar la información de los recursos presentes en la red como la información de usuarios, grupos y políticas de seguridad que se apliquen a éstos.

Red Hat Directory Server simplifica la gestión de usuarios al eliminar la redundancia de datos y automatizar su mantenimiento, mejora la seguridad permitiendo a los administradores de red implementar políticas de control de acceso a la información del directorio y contar con una fuente de autenticación para los recursos de la red y aplicaciones de software empresariales.

Soporta versiones de LDAP2 y LDAP3, operaciones de LDAP v2 y v3, filtros de búsqueda de LDAP incluyendo operadores Booleanos. Soporta referencias de LDAP v3 que permiten a un directorio referir una consulta a otro directorio. Implementa mensajería instantánea con los usuarios del directorio. Incluye índices flexibles a nivel de atributo que permiten optimizar el rendimiento en función del perfil de utilización.

Soporta replicación multi-master hasta 4 servidores por red, restringe el acceso a los datos del directorio mediante el control hasta el nivel de valores de atributo. Controla la capacidad del usuario de realizar operaciones de lectura, escritura, búsqueda o comparación. Provee un control de acceso en función de la identidad del usuario, pertenencia a grupos, identidad de roles, dirección IP, nombre de dominio o normas basadas en patrones.

1.2.2.7. Apache Directory Server.

Es un servidor de directorio complemente escrito en código Java, se lo puede obtener bajo Apache Software, es compatible con LDAP3 certificado por el Open Group, soporta otros protocolos de red tal como Kerberos y NTP, además provee procedimientos almacenados, triggers y vistas características que están presentes en las base de datos relacionales pero no el

mundo LDAP.

1.3. Diferencias entre Active Directory y Dominios Windows NT.

- Los servidores de Dominio NT.4 no tienen la capacidad para soportar varios servidores de dominio de administración principal por segmento de red, en relación con el Active Directory que si soporta este esquema.
- Active Directory ya incorpora el soporte para la implementación de varios servidores secundarios, los cuales tienen su función definida y limitada de permitir solo la lectura de información del Directorio Activo a diferencia de su predecesor Windows NT.
- Los servidores de Active Directory soportan la implementación de varios servidores de Domino Principal en un mismo segmento de red.
- Active Directory integra a esta versión el soporte para la creación de estructuras jerárquicas de sub-dominios.
- Active Directory maneja la degradación de servicios en caliente desde la herramienta DCPROMO a diferencia del Servidor de Domino Windows NT4 que lo realizaba manualmente y era efectiva después del reinicio de los equipos.

1.4. Diferencias entre Active Directory y un LDAP.

- Active Directory es el producto de Microsoft basado sobre el estándar X500.
- Active Directory maneja el acceso directamente con los equipos en la red a diferencia de un servidor de LDAP que lo maneja a través de Samba.
- Active Directory tiene la capacidad de manejar políticas de seguridad centralizadas, a diferencia de un servidor de LDAP que utiliza a Samba para realizar estas tareas.
- Los costos de implementación de un Active Directory aumentan de acuerdo a las funcionalidades contratadas a diferencia de un servidor LDAP que no tiene costo extra por funcionalidades adicionales.
- Active Directory a diferencia de un servidor LDAP no posee la ventaja de ser personalizado de acuerdo a las necesidades de la organización.

1.5. Diferencias entre un Domino Windows NT y LDAP.

- Los servidores de dominio de Windows NT no permiten cambios en el nombre del dominio sin reinstalar el sistema operativo.
- Los servidores de dominio de Windows NT están basados en una única arquitectura de red en la cual solo puede existir un único servidor NT maestro.
- En dominios de Windows NT no pueden coexistir Servidores Principales y Secundarios en el mismo segmento de red.
- En dominios de Windows NT no puede haber controladores de dominio de Windows 2000 server y Windows 2003 server, hasta que sea actualizado el PDC (Servidor de Dominio NT primario) a versiones superiores.
- Una arquitectura de red basadas en tecnologías sobre LDAP y Samba puede coexistir en sus versiones de LDAP v2 y LDAP v3 manteniéndolas operativas.
- Con los Servidores de Dominios basados en los estándares Ldap y Samba la degradación de los servicios se reduce a la modificación del archivo de configuración en la cual se especifica su función sin necesidad de realizar una reinstalación del sistema operativo.
- Un Servidor de Domino de Windows NT no puede contener otros grupos globales o cuentas que pertenezcan a ese domino.
- Con los Servidores basados en tecnologías Open source como son OpenLdap y Samba se pueden administrar más de un Dominio con el mismo directorio Activo.

1.6. Protocolo Ligero de Acceso a Directorios (LDAP).

1.6.1.1. ¿Qué es el LDAP?[4].

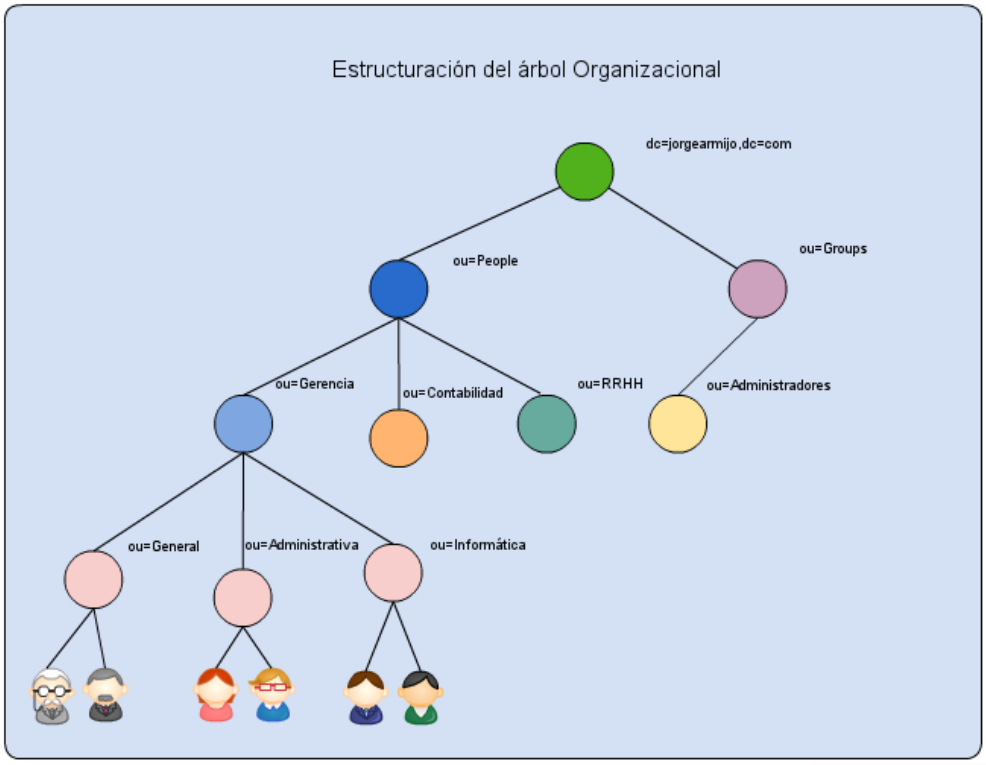
LDAP Lightweight Directory Access Protocol, es un Protocolo Ligero de Acceso a Directorios que está basado sobre protocolos de comunicación TCP/IP, en lo que se refiere a la transferencia de información a través de la red y están definidos por la ITU-T. Puede ser ejecutado sobre cualquier tipo de sistema operativo se basa en los protocolos X.500 que es un conjunto de estándares que se han desarrollado para cubrir las necesidades de administración de la información de forma ágil y precisa de un directorio de acceso ligero.

[4]Addison Wesley – Understanding and Deploying Ldap Directory Services 2Nd Ed 2003, Pág. 63

Está constituido por un conjunto de objetos con atributos organizados de manera lógica y jerárquica, que permiten mantener una estructura ordenada de la información que almacena y que ésta, se ajuste al modelo organizacional de la empresa.

Un árbol de directorio LDAP puede ser estructurado de acuerdo a las especificaciones del organigrama que tenga definida la institución en donde se va a implementar de manera que pueda reflejar el modelo organizacional.

Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS) para estructurar los niveles más altos de la jerarquía (dc=jorgearmijo, dc=com). Conforme se desciende en el directorio pueden aparecer entradas que representan usuarios, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).



1.7. Ventajas en el uso de LDAP.

Permite el acceso a la información contenida en el directorio activo desde cualquier tipo de plataforma o aplicaciones que la empresa use en su negocio.

Los Protocolos de Acceso a Directorios Activos se destacan sobre los tipos de bases de datos por:

- Ser optimizado para la lectura de registros.
- No tienen que pagar por cada conexión de software cliente o por licencia.
- Tiene la capacidad de realizar réplicas del Directorio Activo sin un número específico que las limite.
- Al ser un producto de código abierto muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.
- Dispone de un modelo de nombres globales que asegura que todas las entradas que están almacenadas sean únicas.
- Usa un sistema de información que permite múltiples directorios independientes.
- Funciona sobre los protocoles TCP/IP y SSL para garantizar conexiones seguras al directorio.
- La replicación del directorio puede ser parcial o total.
- Permite la creación de perfiles de cualquier objeto o conjunto de perfiles.
- Implementa varios tipos de replicación para descentralizar los recursos de red.

1.8. Historia del LDAP y estándares utilizados.[5]

Alrededor de la Década de los 70 el desarrollo de las comunicaciones y las tecnologías informáticas llevó a la evolución de nuevos tipos de tecnología. Muchos de los sistemas informáticos desarrollados en esa época eran incompatibles con otros sistemas de lo cual surgió la necesidad de realizar una integración de los distintos proveedores de tecnología en el mercado convergiendo así en el desarrollo de estándares de comunicación.

A finales de la década de los 70 dos organismos de normalización independientes comenzaron a trabajar sobre servicios de directorios, Uno de estos fue el CCITT (Consultative Committee

[5] Addison Wesley – Understanding and Deploying Ldap Directory Services, Segunda Edición 2003, Pág. 48

for International Telegraphy and Telephony) Comité Consultivo Internacional Telegráfico y Telefónico, organismo de las Naciones Unidas encargado de establecer los estándares internacionales sobre telecomunicaciones, actualmente es conocido como ITU. (International Telecommunications Union), Unión Internacional de Telecomunicaciones, para este organismo era importante crear un directorio de páginas el cual podría ser usado para buscar información como nombres, números de teléfono y direcciones de correo electrónico. El otro organismo de normalización era la ISO (International Standard Organization) Organización Internacional de Normalización, que quería un directorio el cual sirva como un servicio de nombres para la OSI (Open Systems Interconnection) Interconexión entre Sistemas Abiertos sus redes y las aplicaciones que se encuentren en estas.

Eventualmente los dos organismos empezaron a trabajar en conjunto y a editar una sola versión de estándares de comunicación, dando inicio a la primera versión del estándar X.500.

En el momento en que fue definido por los años 70, los protocolos X.500 tenían que contemplar los diferentes tipos de información que se debían administrar y que para la época eran novedosos y revolucionarios. En una primera etapa de desarrollo el protocolo X.500 fue uno de los primeros y verdaderos sistemas de directorio con un propósito general definido el mismo que fue diseñado desde el principio para administrar información de personas y el atender las necesidades de una gran variedad de aplicaciones. En una segunda etapa, los protocolos X.500 proporcionan una operación de búsqueda optimizada que agilita el proceso de consultas. En una tercera etapa, los protocolos X.500 fueron diseñados para ser sistemas altamente distribuidos en el que los servidores de datos puedan mantener un servicio alta mente disponible.

El protocolo X.500 es un estándar abierto y que no se encuentra atado a ningún sistema operativo en específico lo que facilita su modificación e implementación en cualquier sistema de red.

1.9. LDAP Estándares.[6]

A lo largo del desarrollo de las Tecnologías de Comunicación se han definido varios estándares, de entre los cuales para LDAP los principales que intervienen en su funcionamiento son los siguientes

La siguiente es una lista de RFCs que se aplican para LDAP Versión 2 y Versión 3.

1.9.1. RFC 1274 The COSINE and Internet X.500 Schema.[7]

Este documento propone un esquema para el uso del Directorio X.500, detalla cómo debe ser el uso para una arquitectura de nombres, para clases de objetos, para los atributos, y un gran número de generalidades que son usadas por las clases de objetos y atributos.

1.9.2. RFC 1777 Lightweight Directory Access Protocol (V2).[8]

El protocolo descrito en este documento está diseñado para proveer acceso al Directorio X.500, además no utiliza todos los recursos requeridos por el Protocolo de Acceso a Directorio (DAP). Este protocolo está específicamente orientado a aplicaciones simples de gestión y a buscadores de aplicaciones que provean accesos sencillos de lectura y/o escritura interactiva al directorio X.500, y tiene la intención de ser un complemento al propio DAP.

1.9.3. RFC 2251 Lightweight Directory Access Protocol (v3).[9]

Está rediseñado para proveer acceso al Directorio X.500. Tomado como referencia de la RFC1777.

Este protocolo está dirigido específicamente a las aplicaciones de administración y de exploración de información que proporcionan acceso interactivo de lectura y escritura a los directorios. Cuando se utiliza con un directorio compatible con los protocolos X.500, éste pretende ser un complemento de X.500 DAP.

---

[6] http://www.ietf.org/

[7] http://www.ietf.org/rfc/rfc1274

[8] http://www.rfc-editor.org/rfc/rfc1777

[9] http://www.rfc-editor.org/info/rfc2251

Los aspectos clave de esta versión de LDAP son:

- Todos los elementos de protocolo de LDAPv2 (RFC 1777) son compatibles. El protocolo se transmite directamente a través de TCP o de otro tipo de transporte, pasando por alto gran parte de la sobrecarga de la sesión de presentación de X.500 DAP.

- La mayoría de los elementos de datos de protocolo se pueden codificar como cadenas normales (por ejemplo, los nombres completos).

- Se pueden devolver referencias a otros servidores.

- Mecanismos de SASL (Simple Authentication and Security Layer – Capa de seguridad y autenticación simple) pueden utilizarse con LDAP para proporcionar servicios de seguridad de la asociación.

- Valores de los atributos y los nombres completos han sido internacionalizados mediante el uso del juego de caracteres ISO 10646.

- El protocolo se puede extender para admitir nuevas operaciones y controles, además pueden utilizarse para ampliar las operaciones existentes.

1.9.4. RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions.[10]

El protocolo descrito hace referencia a la definición de la sintaxis de los atributos utilizados por LDAP y sus aplicaciones, incluyendo la manera como se representan estos valores como en cadenas simples.

El protocolo ligero de acceso a directorios requiere que el contenido de los campos AttributeValue en elementos de protocolo sea cadenas de octetos. En este RFC también se

[10] http://www.rfc-editor.org/info/rfc2252

definen un conjunto de tipos de atributos que deben admitir los servidores LDAP.

1.9.5. RFC 2253 Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names[11]

El protocolo descrito hace referencia a la definición de la sintaxis que se utiliza para la definición de los nombres distinguidos como las claves principales a las entradas del directorio. Los nombres completos se codifican en ASN.1 de los protocolos de directorio X.500.

En Lightweight Directory Access Protocol, se transfiere una representación de cadena de nombres completos. Esta especificación define el formato de cadena para representar los nombres, que está diseñado para proporcionar una representación limpia de nombres completos utilizados.

1.9.6. RFC 2254 The String Representation of LDAP Search Filters.[12]

El protocolo descrito hace referencia a un esquema de representación de filtros de búsqueda LDAP. El protocolo ligero de acceso a directorios define un filtro de búsqueda que se transmite a un servidor LDAP. Algunas aplicaciones pueden encontrar útil disponer de una forma común de representar estos filtros de búsqueda en un formato legible.

1.9.7. RFC 2255 The LDAP URL Format.[13]

El protocolo hace referencia a las definiciones que se realizan en un esquema de localización uniforme de recursos para recuperar información desde un directorio LDAP.

Este RFC reemplaza al RFC1959. En este RFC está presente una actualización al formato de direcciones URL del LDAPv3 y clarifica cómo se resuelven.

Este documento también define un mecanismo de extensión para las direcciones URL de LDAP.

[11] http://www.rfc-editor.org/info/rfc2253
[12] http://www.rfc-editor.org/info/rfc2254
[13] http://www.rfc-editor.org/info/rfc2255

1.9.8. RFC 2256 A Summary of the X.500 User Schema for Use with LDAPv3.[14]

Este documento proporciona una visión general de los tipos de atributos y clases de objetos definidas por los Comités de ISO e ITU-T en los documentos X.500, en particular los destinados a los clientes de directorio. Este es el esquema utilizado con más frecuencia para los directorios LDAP/X.500.

1.9.9. RFC 2829 Authentication Methods for LDAP.[15]

Este protocolo hace referencia a los mecanismos y políticas de autenticación necesaria y opcional que deben soportar los servidores y los clientes para el uso de LDAPv3.

1.9.10. RFC 2830 Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.[16]

El protocolo hace referencia al método de configuración de TLS para mantener la autenticación y privacidad en el LDAPv3.

1.9.11. RFC 2849: The LDAP Data Interchange Format (LDIF)[17]

El formato LDIF se utiliza para transmitir la información del directorio, o una descripción de un conjunto de cambios realizados en las entradas de directorio.

Un archivo LDIF consiste en una serie de registros distanciados por separadores de línea. Un registro se compone de una secuencia de líneas que describen una entrada de directorio, o una secuencia de líneas que describen un conjunto de cambios en una entrada de directorio. Un archivo LDIF especifica un conjunto de entradas de directorio, o un conjunto de cambios que se aplicaran a las entradas de directorio, pero no ambos.

[14] http://www.rfc-editor.org/info/rfc2256
[15] http://www.rfc-editor.org/info/rfc2829

[16] http://www.rfc-editor.org/info/rfc2830
[17] http://www.rfc-editor.org/info/rfc2849

1.10. Diferencias entre un LDAP y una Base de Datos.

Las diferencias marcadas entre un Servidor LDAP y una Base de Datos son:

- Un Servidor Ldap no realiza operaciones de escritura intensivas en comparación con las bases de datos relacionales. Estás se mantienen preparadas para hacer un uso constante de operaciones orientadas a transacciones, que implican la modificación o borrado constante de los datos almacenados.

- En un Servidor Ldap se usa un esquema específico para todas las aplicaciones en comparación con las bases de datos relacionales que son creadas para cada aplicación específica, siendo complicado adaptar los esquemas a nuevas aplicaciones.

- El Modelo de datos manejado en un servidor Ldap no es complejo en comparación con las bases de datos las que permiten manejar complejos modelos de datos que requieren muchas tablas, foreign keys, operaciones de unión complejas.

Sin duda el manejo de la información tanto para los servidores de Base de datos y LDAP mantienen mecanismos de protección similares para procurar mantener la integridad de la información y la consistencia de la misma a todo momento. En ambos incluyen operaciones de rollback, integridad referencial y operaciones orientadas a transacciones.

1.11. Características de un LDAP.

Entre las características más importantes de un LDAP podemos resaltar las siguientes:

1.11.1. Escalabilidad.

La opción de escalabilidad de los Servidores LDAP dependerá únicamente de la restricción de hardware que se disponga en la institución. LDAP tiene la característica de escalabilidad muy elevada al no tener restricción en el número de servidores de réplica.

Los directorios LDAP no dependen de un sistema operativo lo cual maximiza su utilización dando la opción de poder configurar varios sistemas operativos y tener un solo directorio

activo en común al cual se hace referencia.

1.11.2. Disponibilidad.

Al no tener un limitante más que la capacidad de hardware por parte de la configuración de los servidores LDAP estos soportan la réplica a varios servidores que puedan almacenar el mismo contenido del directorio y que nos permite garantizar un esquema de respaldos, además de proveer de una administración descentralizada permitiendo minimizar el consumo de recursos de red. Esto permite a los clientes disponer de estos servidores adicionales cuando alguno de ellos presenta un daño o simplemente se lo aísla del ambiente de producción por algún tema de mantenimiento.

1.11.3. Seguridad.

La seguridad implementada por los directorios LDAP se basa en la autenticación por medio de la capa de conexión segura SSL (Secure Sockets Layer) la cual provee autenticación y privacidad de la información mediante el uso de criptografía. El proceso de autenticación que manejan los directorios activos como OpenLdap estan basados en procesos de verificación de certificados digitales e intercambio de claves públicas entre los clientes y el servidor del directorio activo.

La seguridad se maneja compartiendo recursos propios del esquema del directorio activo, como es las listas del control de acceso ACL (Access Control List) con esto se puede garantizar el máximo nivel de seguridad en el uso de un directorio activo.

1.11.4. Gestionabilidad.

En cuanto a la gestionabilidad de los directorios activos al ser este un proyecto Open Source existen varias herramientas que permiten a los administradores del directorio mantener un control de alto nivel como es a través de la consola de texto, así como también existen herramientas de interfaz gráfica que pueden ser usadas por administradores y usuarios finales que limitan su uso por las ACL y roles administrativos para mantener un manejo granular sobre la administración del directorio activo. Es decir podemos tener varios perfiles de administración del árbol, de esta forma descentralizamos la administración pero maximizamos la opción de sostener al directorio de Información que previamente debe ser instruida para que

no conlleve a tener problemas de inconstancia de datos en el Directorio Activo.

1.11.5. Estandarización.

A través de las Normas "RFC" que se establecen para los Directorios Activos se puede mantener un estándar del tipo de información que se almacenara y los procedimientos de almacenarla y administrarla.

1.11.6. Operaciones de lectura muy rápidas.

Una de las grandes características de los Directorios Activos radica en que la mayoría de los servidores LDAP están fuertemente optimizados para operaciones de lectura intensivas y no para la escritura masiva de registros como sucede con las Bases de datos relacionales. A causa de esto, uno puede notar un orden de magnitud diferente cuando se procede a realizar una consulta de datos a un directorio LDAP frente a la obtención de los mismos Datos de una Base de Datos Relacional optimizada. Por esta razón los directorios activos son usados para almacenar información que pocas veces podrá ser modificada.

1.11.7. Datos relativamente estáticos.

Una de las diferencias notorias en un Directorio Activo es que la información que este contiene no es modificada con regularidad ahí el hecho de crear un directorio activo y no usar un motor de base de datos el cual sería sobre utilizado para las tareas de administración el cual cubre los Directorios Activos. Como por ejemplo las cuentas de correo electrónico de las personas, sus nombres, apellidos, sus claves de autenticación.

1.11.8. Entorno distribuido.

Una de las mayores ventajas que presenta LDAP en comparación con sus competencias directas es la distribución de su servicio en una organización, esto además de reducir costos de implementación de la herramienta proporciona un esquema de respaldos eficiente ya que podemos tener en diferentes lugares geográficos la misma configuración del servicio, y en caso imprevisto de daño del servidor principal este podrá ser reemplazado con cualquiera de ellas garantizando la continuidad del servicio.

1.11.9. Estructura jerárquica.

Los servidores de Directorio Activo mantienen una estructura de almacenamiento jerárquica similar a la estructura de directorios de Unix y al igual que ésta permite la definición de nodos principales y secundarios las cuales establecen políticas de seguridad en diferentes niveles de lo que se conoce más comúnmente como el árbol del Directorio Activo. Para comprender un poco más la estructura que maneja los Directorios Activos LDAP estos se asemejan a las representaciones que se tienen en los DNS. El nivel superior de un Directorio Activo LDAP es la base del Directorio, conocido como "DN base". Un "Distinguished Name" base en inglés o conocido como Nombre Distinguido y viene a definir la cabecera inicial del árbol.

1.12. Arquitectura del LDAP.

1.12.1. Componente de Información.[18]

Define la clase de información puede ser almacenada en un directorio LDAP. Definidos en el RFC2256. Este componente de información hace especial énfasis en las entradas que se realizan en el directorio y la información que estas contienen, recordemos que una entrada está compuesta por atributos las cuales determinan que tipo de objeto es dentro del directorio, y cada uno de estos tiene un tipo y valor específico el cual puede o no servir como campo para relacionarlo con más objetos.

El tipo de un atributo tiene asociado una sintaxis en particular y que define el tipo de información que puede ser almacenada en este atributo, esta definición de atributos influye en el tiempo de respuesta cuando se realiza una búsqueda en el Directorio LDAP. Como por ejemplo un atributo que comparten todos los objetos es el **"cn"** (Common Name) o nombre común en español es el atributo por el cual se identifica al objeto en el directorio LDAP, este atributo tiene una sintaxis llamada "caseIgnoreString" esto significa que tiene un ordenamiento lexicográfico, y que tiene que almacenar valores en cadena de caracteres, El atributo telephoneNumber tiene una sintaxis idéntica a la sintaxis caseIgnoreString, salvo que se ignoran los espacios y guiones durante las comparaciones. Esto permite que los valores tales como "593-2295153" y "5932295153" se consideren equivalentes.

Los tipos de atributos también pueden tener diversas limitaciones asociadas con ellos, como

[18] Steven Tuttle, Ami Ehlenberger. Understanding LDAP Design and Implementation, International Technical Support Organization, Segunda Edición Junio 2004, Pág. 56

puede ser en número de valores que pueden almacenar o el tamaño de esos valores. Por ejemplo, un atributo que contenga el número de identificación de una persona podrá ser un valor único y limitado por una cantidad específica de valores. Otro ejemplo puede ser el atributo que contenga una fotografía y el limitante para este sería el tamaño para evitar que se use un excesivo espacio de almacenamiento.

Los atributos son controlados por las reglas de contenido establecidas en los ObjectClass. Los valores de estos atributos identifican el tipo de entrada en el directorio como personas, equipos, organizaciones, etc. Los ObjectClass permiten determinar que atributos son obligatorios y cuales son opcionales para cada objeto del directorio LDAP. Por ejemplo, el ObjectClass de un objeto persona requiere los atributos sn (por apellido) y cn (por nombre común), y permite la descripción del objeto persona. Esto es equivalente a los esquemas que se utilizan en las bases de datos relacionales.

1.12.2. Componente de Nomenclatura.[19]

Define como la información en un directorio LDAP puede ser organizada y referenciada.

Aunque no es un requisito del protocolo LDAP, las entradas se colocan generalmente en una estructura de árbol que sigue una distribución geográfica, organizativa o una mezcla de ambas esto depende de las necesidades de las organizaciones en explotar en su mayor capacidad las ventajas de utilizar el modelo jerárquico del LDAP. Las entradas se denominan de acuerdo con su posición en la jerarquía por un nombre distinguido (DN). Cada componente de la rama principal del DN se llama un nombre completo relativo (RDN) y se compone de uno o más atributos de la entrada.

Para cualquiera que está familiarizado con un sistema jerárquico de archivos, tales como los proporcionados por Windows o UNIX, este concepto es fácil de entender. El RDN es similar al nombre del archivo y el DN es similar a la ruta de acceso absoluta al archivo. Al igual que con un sistema de archivos, entradas de nodos hermanos (las entradas con el mismo padre) deben tener diferentes RDN.

[19] Steven Tuttle, Ami Ehlenberger. Understanding LDAP Design and Implementation, International Technical Support Organization, Segunda Edición Junio 2004, Pág. 66

1.12.3. Componente Funcionalidad.[20]

Define las acciones que se pueden realizar con un directorio LDAP y como esta debe ser ingresada y actualizada.

Una vez ya conocido que tipo de información puede ser almacenada en un directorio LDAP y como esta información está organizada y referenciada es hora de comprender las funciones que se pueden realizar con ellas.

Las operaciones en un directorio LDAP las podemos resumir en tres áreas principales:

- ***Consulta: Búsqueda, Comparación***

  Estas operaciones son usadas para realizar consultas de entradas en los directorios. La operación de consulta se utiliza para seleccionar las entradas de un área definida del árbol basándose en algunos criterios de selección conocidos como un filtro de búsqueda.

- ***Actualización: agregar, eliminar, modificar, modificar RDN***

  Estas operaciones son usadas para actualizar información en las entradas de los directorios. La operación de modificación se utiliza para cambiar los atributos y valores contenidos en una entrada existente. La operación de adición se utiliza para insertar una nueva entrada en el directorio. La operación de eliminación se utiliza para eliminar una entrada existente en el directorio. La operación de modificación del RDN se utiliza para cambiar el nombre de una entrada.

- ***Autenticación: Ingreso Salida***

  Estas operaciones son usadas como principio de protección de la información del directorio. Definen una de las operaciones más usadas en un directorio LDAP, permite a un cliente probar su identidad en el directorio. El cliente proporciona un DN de identificación y una contraseña. El servidor no prueba su identidad al cliente. Si no se requiere autenticación, el cliente puede especificar un DN y una contraseña NULL para estos casos. La operación de desvinculación se utiliza para terminar una

[20] Steven Tuttle, Ami Ehlenberger. Understanding LDAP Design and Implementation, International Technical Support Organization, Segunda Edición Junio 2004, Pág. 71

sesión de directorio. Una operación de abandono también se define, lo que permite una operación en curso de ser cancelada.

1.12.4. Componente de Seguridad.[21]

Define como la información en un directorio LDAP puede ser protegida de accesos no autorizados. El modelo de seguridad de los directorios LDAP se basa en conocer la identidad de los clientes que solicitan acceso al directorio. Esta información es proporcionada por la operación de autenticación. Esto es una ventaja para el desarrollo de las aplicaciones que son libres de diseñar el sistema más adecuado para sus necesidades de conexión con el directorio para realizar consultas y obtener la autenticación en el Directorio. En la versión LDAPv3 se implementan varios métodos de autenticación que no están disponibles en las versiones anteriores del protocolo. Algunas funciones, como las listas de control de acceso, no se han normalizado todavía, dejando a los proveedores de servicios esta tarea.

1.13. Arquitectura Cliente – Servidor del servicio de Directorio.

La arquitectura Cliente – Servidor se basa principalmente en una de las características de los directorios LDAP. Es la adaptabilidad que presentan los Directorios LDAP para que varias aplicaciones adquieran información de este servicio. Permite a las empresas u organizaciones ampliar sus capacidades del negocio brindando acceso a la información del directorio de forma única atreves de interfaces fáciles de manejar para los usuarios sin dejar de lado las políticas de seguridad lo que permite implementar procedimientos de autenticación permitiendo acceder a los usuarios a través de una sola interface a varios servicios y a información específica esto se conoce como single sing-on (SSO) o en español se conocería como un sistema centralizado de autenticación y autorización.

[21] Steven Tuttle, Ami Ehlenberger. Understanding LDAP Design and Implementation, International Technical Support Organization, Segunda Edición Junio 2004, Pág. 77

1.14. Directorios Distribuidos.

Una de las principales características que nos ofrece un Directorio Activo es la de mantener directorios distribuidos ya que permite configurar un esquema de Servidores Principales y Secundarios en la misma red con la finalidad de salvaguardar nuestro servicio de Directorio Activo siempre en funcionamiento y disponible para los usuarios finales, con este esquema de Directorios LDAP podemos descentralizar las peticiones que se realizan a un solo equipo como sucede con los modelos centralizados. Para el desarrollo de la guía se ha considerado que mantener un servicio de directorio distribuido es la mejor opción que se puede implementar en una empresa u organización, por esta razón se tomara como ejemplo práctico en esta guía, con este esquema de servidores se puede disponer de varios servidores proporcionando el servicio de directorio y pueden coexistir servidores principales y secundarios. Una de las mayores ventajas cuando el servicio de directorio se encuentra en el esquema distribuido es que el impacto cuando se planifica un mantenimiento de los equipos no es perceptible para los usuarios finales esto debido a que los datos se encuentran replicados en todos sus servidores sean estos principales o secundarios.

1.15. Seguridad del directorio.

1.15.1. Autenticación Anónima.[22]

Es el proceso de conexión con el Servidor de Domino mediante la cadena de texto en la que identifica al usuario y el Dominio con una contraseña vacía. Esta forma de autenticación es muy común, es frecuentemente utilizado por las aplicaciones de cliente, de esta forma facilita mantener la información disponible para las aplicaciones que consuman la información de un Directorio activo.

Por ejemplo una cadena de conexión es la siguiente dc=ejemplo,dc=com

1.15.2. Autenticación Básica.[23]

Es el proceso de conexión con el Servidor de Domino mediante el nombre de usuario en la forma de un DN el cual se envía con una contraseña en texto plano. El Servidor de Domino

[22] Gerald Carter. LDAP System Administration, Primera Edicion, Marzo 2003 Pág. 25
[23] Gerald Carter. LDAP System Administration, Primera Edicion, Marzo 2003 Pág. 25

realiza el procedimiento de validar esta contraseña con el valor userPassword, almacenado. Por seguridad se acostumbra que la contraseña se almacene en un tipo de hash encriptado, el servidor debe generar el hash de la contraseña transmitida y compararlo con la versión almacenada para permitir el acceso.

1.15.3. SSL and TLS[24]

Hay dos formas de utilizar SSL / TLS con LDAPv3:

LDAP sobre SSL (LDAPS - tcp/636) está bien apoyado por muchos servidores LDAP, tanto de origen comercial y de código abierto. Aunque se usa con frecuencia, se ha reducido a favor de la operación prolongada LDAP StartTLS.

El RFC 2830 introdujo una operación extendida LDAPv3 para TLS negociación sobre el puerto estándar tcp/389. Esta operación, que se conoce como StartTLS, la cual permite a un servidor para apoyar las dos sesiones disponibles como cifrados y no cifrados en el mismo puerto, en función de las peticiones de los clientes. Con la excepción de la capa de negociación de seguridad de transporte, el proceso de unión es el mismo que para la autenticación simple.

1.15.4. SASL.[25]

SASL es un esquema de seguridad extensible el que se define en la RFC 2222 y es usada para agregar mecanismos de autenticación adicionales para protocolos orientados a la conexión, tales como IMAP y LDAP. En esencia, SASL es compatible con un esquema de autenticación conectable al permitir que el cliente y el servidor negocien el mecanismo de autenticación antes que se realice la transmisión de las credenciales del usuario. Además de negociar un mecanismo de autenticación, los equipos que se comunican también pueden negociar a nivel de una capa de seguridad más baja como SSL y TLS las cuales se usan para cifrar los datos durante la sesión. RFC 2222 define los varios esquemas de autenticación para SASL, incluyendo:

Kerberos v4 (KERBEROS_V4)

[24] Gerald Carter. LDAP System Administration, Primera Edicion, Marzo 2003 Pág. 34
[25] Gerald Carter. LDAP System Administration, Primera Edicion, Marzo 2003 Pág. 35

La interfaz Generic Security Service aplicación del programa, versión 2 (GSSAPI), que se define en el RFC 2078.

El mecanismo de S/Key o conocido como llave segura, es un sistema de contraseña basado en un solo algoritmo MD5.

El mecanismo externo que permite que una aplicación haga uso de las credenciales de un usuario proporcionado proporcionada por los protocolos SSL / TLS. Además de estos, RFC 2831 ha añadido un mecanismo de SASL/DIGEST-MD5. Este mecanismo es compatible con HTTP/1.1.

Durante el proceso de enlace, el cliente pide al servidor información de las credenciales de identificación para procesar su solicitud mediante un SASL particular. El cliente y el servidor se realizan los pasos adicionales necesarios para validar las credenciales del usuario. Una vez que se ha alcanzado un el acceso una revocatoria del acceso, el servidor devuelve una respuesta a la solicitud de enlace del cliente. En el caso de ser aceptada la solicitud de acceso este se realiza con el mismo procedimiento de validación que en el caso de la Autenticación Básica.

1.16. Información que se almacena en un LDAP.

1.16.1. Entradas.

Una entrada es llamada a la colección de atributos que almacenan información en un Directorio Activo los cuales tienen un único nombre distintivo "DN", cada atributo de una entrada posee un tipo de valores y a una sintaxis específica.

Los nombres distintivos están asignados en palabras nemotécnicas las cuales nos ayudan a que los atributos puedan ser identificados de mayor facilidad. Se han simplificado sus nomenclaturas de forma que utilizando los primeros caracteres de las palabras compuestas como por ejemplo "cn=nombre común" se pueda tener una idea del tipo de información almacenara ese atributo, en ciertos Como por ejemplo "mail=correo electrónico" se usa su palabra completa.

La sintaxis de cada atributo depende del tipo de atributo y este está definido de tal manera que si se ingresa información que no es relacionada con el tipo de sintaxis asignada a el tipo de atributo esto lleva a almacenar información no valida en el Directorio activo y como resultado

se obtiene un tipo de Directorio Activo con errores de sintaxis lo que ocasionaría a posterior inconsistencia en la Información contenida en el Directorio Activo.

1.16.2. Objetos.[26]

Los objetos están definidos en el Directorio Activo como una colección de atributos que pueden usarse para definir una entrada.

Los objetos dentro de un Directorio Activo pueden ser:

- Grupos en el directorio, entre ellos listas no ordenadas de objetos individuales o de grupos de objetos
- Emplazamientos como ejemplo el nombre de su ubicación geográfica y su descripción
- Organizaciones que se consideren en el Árbol del Directorio Activo
- Personas que se encuentren en el Directorio.
- Equipos informáticos que se encuentren en el Directorio.

Una entrada determinada puede pertenecer a más de una clase de objetos, por ejemplo la entrada descrita para la persona se encuentra definida en la clase de objetos "person", pero también puede pertenecer a otros objetos como "inetOrgPerson", "groupOfNames".

1.16.3. Atributos.[27]

Los atributos en un Directorio Activo vienen a ser las características específicas que detallan un objeto, estas pueden variar de los tipos de objetos y mantienen una sintaxis específica para cada uno como por ejemplo un "usuario" como se le conoce al objeto que representa a una persona dentro del directorio activo y presenta varios tipos de atributos que permiten diferenciar un usuario de otro como por el ejemplo el nombre, apellido, la cedula, teléfono, la dirección de su domicilio, estos pueden compartir atributos con los mismos valores es decir pueden compartir atributos que los referencien a un objeto como por el ejemplo el "Gid number" que significa el numero de un grupo que se haya definido. Es decir un atributo puede hacer referencia a otro atributo que describa otro objeto.

Cada atributo tiene la definición de sintaxis que le corresponda. La definición de sintaxis

[26] Daniel E. House, Tim Hahn. E-Directories Enterprise Software, Solutions, and Services, Addison-Wesley, Primera Edicion Julio 2000. Pág. 186

[27] Daniel E. House, Tim Hahn. E-Directories Enterprise Software, Solutions, and Services, Addison-Wesley, Primera Edicion Julio 2000. Pág. 184.

describe el tipo de información que proporciona ese atributo, entre los más utilizados podemos detallar:

- Bin De tipo binario.
- Ces Cadena de caracteres con diferenciación entre mayúsculas y minúsculas.
- Cis Cadena de caracteres que no hace diferenciación entre mayúsculas y minúsculas.
- Tel cadena de números asignada para almacenar los números telefónicos se ignoran los espacios en blancos y caracteres especiales

1.16.4. Tipos de Atributos.

Existe la diferenciación de los atributos que son asignados a un objeto en un Directorio Activo. Estos atributos están identificados como:

1.16.4.1. Atributos Obligatorios.

Los atributos Obligatorios son los tipos de atributos que son necesarios para diferenciar a los objetos entre ellos como por ejemplo se considera obligatorio al atributo de "uid" este atributo es el nombre como se identificara al objeto dentro del Directorio Activo, el "gid", es el atributo que determina a que grupo en particular creado en el Directorio Activo es asignado.

1.16.4.2. Atributos Opcionales.

Los atributos Opcionales son los tipos de atributos que no son necesarios para diferenciar a los objetos entre ellos como por ejemplo el teléfono se considera un tipo de objeto más del tipo informativo que del tipo obligatorio el cual nos puede ayudar a diferenciar a los objetos entre ellos.

1.16.5. Atributos de Objetos más usados.

Entre los atributos más utilizados dentro de un Directorio Activo podemos resumirlos:

Función	**ObjecClass**	**Atributos**	**Descripción**	**Valor por defecto**
User Accounts – Cuentas de Usuarios	Top	Ou	Unidad Organizacional	Usuarios
	Person	Uid	Nombre de uid de unix	Jorge
		Cn	Nombre común	Jorge Armijo
		Sn	Apellido	Armijo

	Account		Propietario tiene una cuenta única	
	posixaccount		Propietario tiene una cuenta del sistema unica	
		UidNumber	Uid Numero de Identificación del Usuario	513
		gidNumber	Gid Número de Identificación del Grupo primario al que pertenece.	100
		Homedirectory	Directorio personal único	/home/jorgearmijo
		Userpassword	Contraseña del usuario para ingresar al Dominio.	P45sW0rD
	Sambaacoount	Ntpasswd	NT password	P45sW0rD
		loginhell	User Shell	/bin/bash
Machine Accounts – Cuentas de maquinas	top	ou	Unidad Organizacional	maquinas
	posixaccount	uid	Nombre de ingreso	ventanilla01$
		uidnumber	Unid uid	516
		gidnumber	gid	200

1.16.6. Esquemas.[28]

Un esquema es un conjunto de reglas que determinan que datos se pueden almacenar en una base de datos si habláramos de un motor de base de datos como SqlServer Oracle Postgres o de un directorio activo. Los esquemas son importantes porque ayudan a mantener la integridad y la calidad de los datos almacenados en un servicio de directorio. Los esquemas también ayudan a reducir la duplicación de datos y proporcionar una forma bien documentada, previsible para las aplicaciones habilitadas para directorios para acceder y modificar la colección de objetos de directorio.

Un esquema de un directorio LDAP es un conjunto de reglas que determinan lo que se puede almacenar en un servicio de directorio y como servidores de directorios y los clientes deben tratar a la información durante las operaciones de directorio, como búsquedas. Antes de que un servidor de directorio almacene una entrada nueva o modificada, comprueba el contenido de la entrada contra de las reglas de esquema. Siempre que los clientes o servidores de directorio

[28] Addison Wesley. Understanding and Deploying Ldap Directory Services, Segunda Edicion 2003 Pág 277

comparan dos valores de atributos, consultan el esquema para determinar que algoritmo de comparación se ha de usar.

Los esquemas también pueden utilizarse para imponer restricciones sobre el tamaño, alcance y formato de los valores de los datos almacenados en el directorio. Por ejemplo, de acuerdo con los estándares de correo de Internet, los valores de dirección de correo electrónico deben utilizar un conjunto restringido de caracteres y deben ajustarse a un formato específico (addr@dominio). En muchos casos, las reglas de esquema imponen restricciones simples, "como este valor debe ser un entero". Asegurarse de que los valores de datos en el servicio de directorio se ajustan a una colección de reglas simples aumenta la calidad, consistencia e integridad de los datos en los directorios LDAP.

1.16.7. Tipos de Esquemas de un LDAP.[29]

Los tipos de esquemas de un Directorio Activo dependen de las necesidades de la Empresa u Organización que implemente esta solución informática, esta puede ser simple o compleja ya depende de las necesidades que se presenten.

El modelo de esquema básico para un directorio Activo está definido en el RFC 2252, y de este podemos guiarnos para obtener información para desarrollar un esquema que cubra necesidades particulares.

Una de las ventajas que destacan a los Protocolos de Acceso a los Directorios Activos como Openldap es que admite múltiples esquemas de información en el directorio permitiendo a las aplicaciones el ingresar información específica de cada negocio haciendo más detallada la información de la organización.

Una de las razones para mantener varios esquemas de información es que las aplicaciones que se desarrollen siempre tendrán características únicas esto permite que las aplicaciones permitan ser actualizadas y mejoradas constantemente de acuerdo a los requerimientos en el tiempo.

Por ejemplo se puede desarrollar una aplicación de control de equipos en la cual se podría integrar el esquema básico de información del Directorio Activo (RFC 2252) con el esquema de Samba usado para la autenticación de equipos y de esta manera poder obtener información

[29] Daniel E. House, Tim Hahn. E-Directories Enterprise Software, Solutions, and Services, Addison-Wesley, Primera Edicion Julio 2000. Pág 173

de las credenciales del equipo que está asociado a un empleado en la organización.

Otro ejemplo puede ser aplicado al departamento de recursos humanos en el cual se pretenda desarrollar una aplicación para incrementar la información de cada empleado como el estado civil de esta persona, la fecha de nacimiento, si tiene hijos o no, las edades de ellos, dirección del domiciliaria, teléfonos, información médica, alergias del empleado en fin sin número de información dependiendo de las necesidades del negocio en general que puedan ser tabuladas en un sistema informático.

1.16.8. Archivos LDIF.[30]

Los Archivos con extensión LDIF hacen referencia al formato de intercambio de datos de los directorios LDAP formato basado en texto estándar para describir las entradas de directorio, que se define en el RFC2849. El formato de archivos LDIF permite exportar los datos del directorio, e importarlo en otro servidor de directorio, esta es la manera más práctica de obtener respaldos de los directorios LDAP.

1.17. Estructura de la Información dentro del LDAP.

La estructura de un Directorio Activo está organizada de forma jerárquica, se lo considera como un tipo especial de base de datos. Los directorios activos están optimizados para admitir un gran volumen de solicitudes de lectura junto con el acceso de escritura. El objetivo de realizar esta optimización es que un directorio activo realiza más peticiones de lectura de información que la actualización de la misma. Podemos hacer una analogía con una guía telefónica, pero con más información sobre cada atributo que se muestre definido.

1.18. Indexación de la Información de un LDAP.

La indexación de atributos nos permite realizar búsquedas de información al directorio activo de una forma más rápida y ágil como es una de las características principales de los directorios activos, la indexación de atributos se la define en el archivo de configuración del OpenLdap, en este archivo de configuración podemos definir como índices de búsqueda el CN o Nombre Común, el mail, uid, para el tipo de objeto users o usuarios por medio de la indexación

[30] Addison Wesley – Understanding and Deploying Ldap Directory Services 2Nd Ed 2003, Pág. 101

podemos hacer que la búsqueda de información sea más ágil y rápida y estará ligada directamente a la cantidad de atributos que se definan para la indexación.

1.19. Filtros de búsqueda en LDAP.

Los filtros de búsqueda en los directorios activos son los atributos que fueron declarados como requeridos en el esquema definido para el directorio activo, entre los filtros de búsqueda más comunes están:

- ***UID***: identificador único del objeto.
- ***MAIL***: correo electrónico.

Para mejorar el tiempo de respuesta en la búsqueda de información se requiere que los campos a ser buscados estén indexados en el directorio.
Para el desarrollo de esta guía metodológica utilizaremos el esquema que está definido por defecto en la instalación del OpenLdap.

1.20. Estándar sistemas x.500.[31]

El protocolo X.500 es un estándar abierto no controlado por ningún proveedor y que no se encuentra atado a ningún sistema operativo en específico lo que facilita su implementación, modificación en cualquier sistema de red.
En la década de 1980, dos organismos de normalización independientes comenzaron a trabajar en forma autónoma sobre los servicios de directorio que indistintamente requerían. El CCITT, que más tarde cambió su nombre por el de ITU se concentró en analizar y crear un estándar que permitiera realizar la búsqueda de información básica como nombres de contactos, teléfonos, correos electrónicos de forma ágil y simple. El OSI buscaba como proveer un servicio de nombres para la interconexión de sistemas abiertos como redes y aplicaciones.
Con el fin de satisfacer esta creciente necesidad a mediados de 1988 se procedió a desarrollar un conjunto de definiciones para un servicio de directorio genérico llamada Familia X.500 y

[31] Daniel E. House, Tim Hahn. E-Directories Enterprise Software, Solutions, and Services, Addison-Wesley, Primera Edicion Julio 2000. Pág 78

se lo público a inicios de 1990, que se actualizo posteriormente en 1993, 1997 y 2001.
Entre ellas podemos mencionar las más importantes:

- ***X.501: Los Modelos de información.*** Describe los conceptos y modelos que son la base un servicio de directorio X.500.

- ***X.509: Normas de autenticación.*** Describe en detalle cómo se maneja la autenticación de los clientes y servidores de directorio en X.500.

- ***X.511: Definición de Servicios.*** Describe en detalle los servicios funcionales prestados por los directorios X.500 por ejemplo, operaciones de búsqueda, de adición, de eliminación, de modificación.

- ***X.518: Procedimientos para operación distribuida***. Describe cómo se manejan las operaciones de directorio que abarcan múltiples servidores, entre otros detalles.

- ***X.519: Especificaciones de protocolo.*** Describe todos los protocolos X.500, incluyendo Directory Access Protocol (DAP), Directory System Protocol (DSP), Directorio de Protocolo de enlace operacional (DOP) y la información del directorio del remedo Protocol (DISP).

- ***X.520: Tipos de atributos seleccionados.*** Define los tipos de atributos X.500 utilizados por sí mismo, y algunos que son generalmente útiles (tal como el atributo telephoneNumber).

- ***X.521: Clases de objetos seleccionados.*** Define las clases de objetos utilizados por X.500 sí, y algunos que por lo general son útiles también (como la clase de objetos person).

- ***X.525: Replicación***. Describe cómo se replica el contenido del directorio entre X.500 servidores.

- ***X.530: Sistemas de Gestión*.** Describe cómo un servicio de directorio X.500 se puede gestionar a través de la utilización de los servicios de inspección in situ los sistemas de gestión y protocolos, servicios y protocolos de directorio, y los medios locales.

1.21. Diferencia entre versiones del LDAPv2 y LDAPv3.

La versión de LDAP 3 incorpora cambios significativos en comparación con su predecesora como se describe a continuación:

- La administración de los servicios se maneja vía SASL aumentando la seguridad en la autenticación.

- Se procedió a incorporar certificados de autenticación a través de TLS (SSL) para proteger la integridad y confidencialidad de la información que se almacena.

- Cambio en la administración del esquema definido en el directorio a partir de esta versión el esquema puede ser modificable de acuerdo a las necesidades para la creación de nuevos atributos o modificación de los existentes.

- Se estandarizo el uso de caracteres especiales "unicode" para facilitar el ingreso de la información apegándose a los estándares establecidos por " Unicode Technical Committee" asignando un único número para cada carácter sin importar la plataforma, ni el programa, ni el idioma, permitiendo un fácil traspaso entre distintos sistemas de codificación y plataformas.

- La versión de LDAP 3 implementa la replicación desde varios servidores Principales a varios servidores secundarios.

1.22. Protocolos de Sincronización LDAP.[32]

La sincronización es el proceso en el que los cambios realizados en el servidor principal se ven reflejados en los servidores secundarios. La sincronización se realiza normalmente con frecuencia (cada hora, día o semana dependiendo del uso del directorio), la sincronización se puede realizar en una o ambas direcciones y entre dos o más fuentes de datos.

El protocolo de sincronización y replicación de LDAP, syncrepl para abreviar mantiene la sincronización de la información del directorio activo y esta se realiza desde los servidores secundarios hacia el servidor primario a través del puerto 398 definido en el archivo de configuración del OpenLDap slapd.conf.

La sincronización del directorio activo permite a los servidores secundarios mantener una copia instantánea del directorio global o a su vez este se puede configurar para que se sincronice solo un fragmento del directorio en caso de ser necesario.

1.23. Tipos de Sincronización y Replicación.[33]

Dependiendo de la disposición de los servidores principales y secundarios en la infraestructura de Red OpenLdap suministra dos métodos para realizar la Sincronización y la Replicación. El primero se realiza a través de los demonios de slurpd y slapd, los cuales observan los cambios en el servidor principal y conduce los mismos a los servidores secundarios. El segundo utiliza el motor de replicación de sincronización de LDAP conocido como syncrepl, a continuación detallaremos el funcionamiento de cada uno.

1.23.1. Sincronización y Replicación con slurpd, slapd.

Estos demonios se configuran sobre el servidor LDAP principal y se encargan de realizar las tareas de sincronización y replicación hacia los servidores LDAP secundarios, el estado de las últimas tareas de sincronización y replicación realizadas se almacena en el servidor principal. Este proceso era considerado bastante inestable razón por la cual en la última versión de LDAP se corrigió este mecanismo de replicación.

El flujo de los datos en el modelo de replicación slurpd inicia desde el cliente el que realiza la

[32] Addison Wesley. Understanding and Deploying Ldap Directory Services, Segunda Edicion 2003 Pág 271
[33] Ian Clatworthy. OpenLDAP Software 2.4 Administrator's Guide, The OpenLDAP Foundation, All Rights Reserved. Cuarta Edición Pág. 163

petición de información buscando este su servidor principal más próximo el que administra todas las escrituras del directorio activo. Cualquier cambio al árbol del servidor principal es ingresado en un registro de replicación, el cual es monitoreado por el demonio slurpd. Tras previa notificación de un cambio en el registro de replicación del servidor principal el demonio slurpd impulsa los cambios a todos los servidores esclavos descritos en el archivo de configuración slapd.conf

1.23.2. Sincronización y Replicación con SynRepl.

La forma de envió de información usada por slurpd conocida también como "push" o "empuje" en español a su tiempo fue una solución sencilla para el problema de la replicación entre servidores LDAP, slurpd dio buenos resultados en su momento.

De acuerdo al RFC 4533 el cual describe la operación de sincronización de contenido de LDAP, es implementada por OpenLDAP con el motor de replicación y de sincronización LDAP, también conocido como syncrepl.

Es el nuevo tipo de sincronización implementada desde la tercera versión de LDAP en reemplazo de los demonios de sus versiones previas.

Sobre este tipo de sincronización se tienen dos diferenciaciones:

- Empuje de información bajo petición. En este se realiza solo la actualización del directorio por pedido del servidor secundario que se conecta periódicamente al servidor principal en busca de cambios en el directorio desde la última conexión realizada por este. El servidor secundario solicita una cookie que mantiene el rastro del último cambio sincronizado y luego se desconecta, la forma de actualización parte a raíz de la descarga de este archivo en el cual la cookie se presenta al servidor principal el que contiene información de las entradas de información que cambiaron desde la última sincronización.

- Refresco de información permanente. Inicia como el método anterior pero en el cual el servidor principal está enviando permanentemente los cambios hacia los servidores

secundarios que a diferencia con el método anterior este nunca cierra la conexión con el servidor principal.

1.24. Replicación.[34]

En versiones anteriores a LDAP 3 la sincronización y replicación de la información de un servidor principal hacia los servidores secundarios se realizaba por medio de los demonios de slurpd y slapd, entre las mejoras implementadas en la última versión de LDAP y con la cual se desarrollara la guía metodológica se incorpora el soporte para la replicación hacia múltiples servidores principales y varios servidores secundarios, incrementando la fiabilidad y la integridad de la información del directorio activo. Sin embargo para este tipo de servicio en el cual el trabajo de personas depende de la disponibilidad del mismo se considera que el porcentaje de tolerancia a fallas debe ser del 0%, el cual se cumple por medio de una estrategia de replicación. En este caso en particular para el servidor de domino OpenLdap la configuración para la replicación se la puede realizar de varias formas entre las cuales las más conocidas son **"Maestro – Maestro" o "Maestro – Esclavo"** y que técnicamente se consideran estrictamente necesarias como un método de respaldo de información del directorio.

Es llamado servidor LDAP principal o maestro, cuando sobre este se mantiene activado la lectura y escritura de información y es el encargado de mantener la última versión del directorio activo.

Es llamado servidor LDAP secundario o esclavo al servidor que realiza las peticiones de sincronización y actualización de la información a un servidor LDAP principal.

Para tener una mejor idea del concepto del esquema de servidores Maestro – Esclavo en la organización o empresa podemos decir que el servidor LDAP principal es quien recepta la información y puede ser de diversas formas como a través de herramientas web que están disponibles para los usuarios y la línea de comandos para realizar tareas administrativas. En este esquema en los servidores llamados esclavos, secundarios o conocidos también como servidores consumidores de información son los que mantienen una copia idéntica de la estructura del árbol del servidor maestro y las aplicaciones o personas pueden realizar tareas

[34] Ian Clatworthy. OpenLDAP Software 2.4 Administrator's Guide, The OpenLDAP Foundation, All Rights Reserved. Cuarta Edición Pág.159.

solo de lectura de información de estos.

Con todos los antecedentes mencionados se considera que la replicación de la información se ha convertido en un requisito indispensable para el flujo continuo del negocio por lo que se puede identificar cuatro razones principales por lo cual debemos tener un esquema de replicación en la empresa u organización y son:

- ***La Confiabilidad***

  La confianza de mantener un servicio de esta naturaleza es crítico debido a la información que provee a usuarios y aplicaciones por lo que se considera indispensable contar con al menos un servidor maestro o esclavo como respaldo del principal.

- ***La Disponibilidad***

  El factor de tolerancia de mantener un servicio disponible 24x7 y más aún el directorio sobre el cual se permite el ingreso a las aplicaciones de la empresa se convierte en un punto crítico del negocio y es seguro que no es discutible la disponibilidad por lo cual es indispensable combinar un esquema de replicación con un esquema de respaldos del directorio y sus configuraciones.

- ***La Localidad***

  Tener disponible un servidor de respaldo en la misma localidad reducirá el tiempo de impacto sobre mantenimientos planificados del hardware sobre el cual está la configuración del servidor LDAP principal.

- ***El Rendimiento***

  Al mantener esquemas distribuidos de servidores principales se reducirá el tiempo de atención sobre la carga de peticiones de información manteniendo un balanceo de tráfico hacia los equipos configurados como servidores principales.

OpenLdap será el Software de Directorio Activo que se escogerá en el desarrollo de esta guía metodológica ya que soporta varias estrategias de replicación las cuales son:

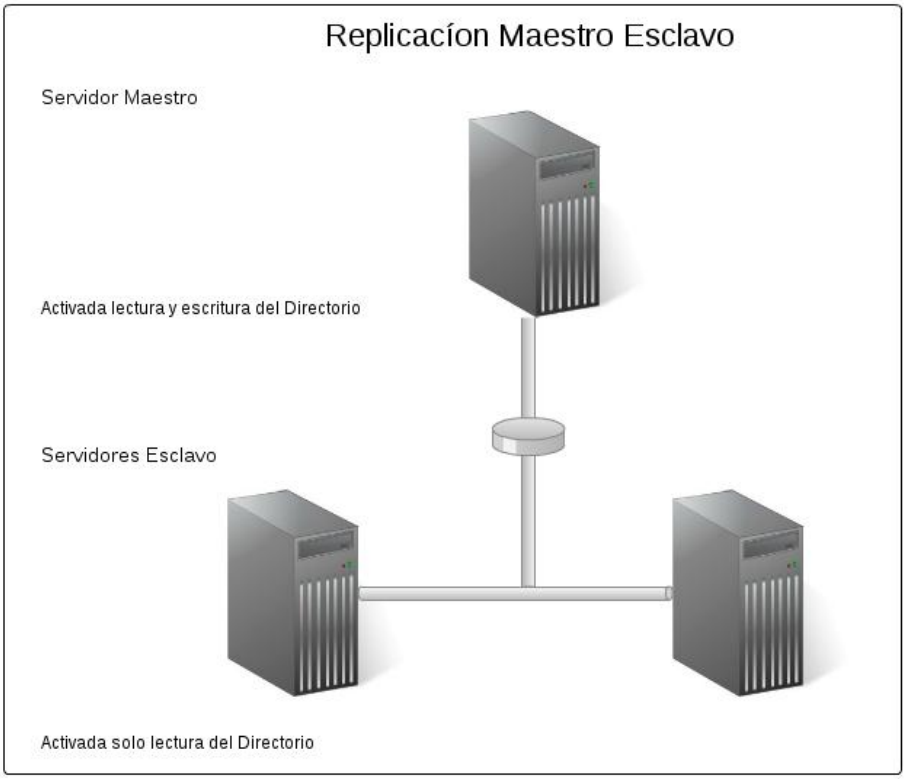
1.24.1. Replicación Maestro – Esclavo.

En este esquema de replicación se realiza la configuración de un solo servidor como principal o maestro el cual tiene la característica principal de ser el único sobre el cual tiene habilitado la escritura en el directorio, los demás servidores en la red serán los servidores replicas o secundarios los cuales se mantienen actualizados cada cierto tiempo.

Este modelo de replicación se utiliza para optimizar el recurso de servicios en la red como puede ser el acceso a aplicaciones o para la autenticación sobre equipos en un controlador de dominio primario de red.

Este tipo de modelo es muy útil cuando en una organización se dispone de usuarios en diversas localidades y que deben de acceder al mismo repositorio de información para validación de cuentas en estaciones de trabajo o a su vez para validar el acceso a aplicaciones.

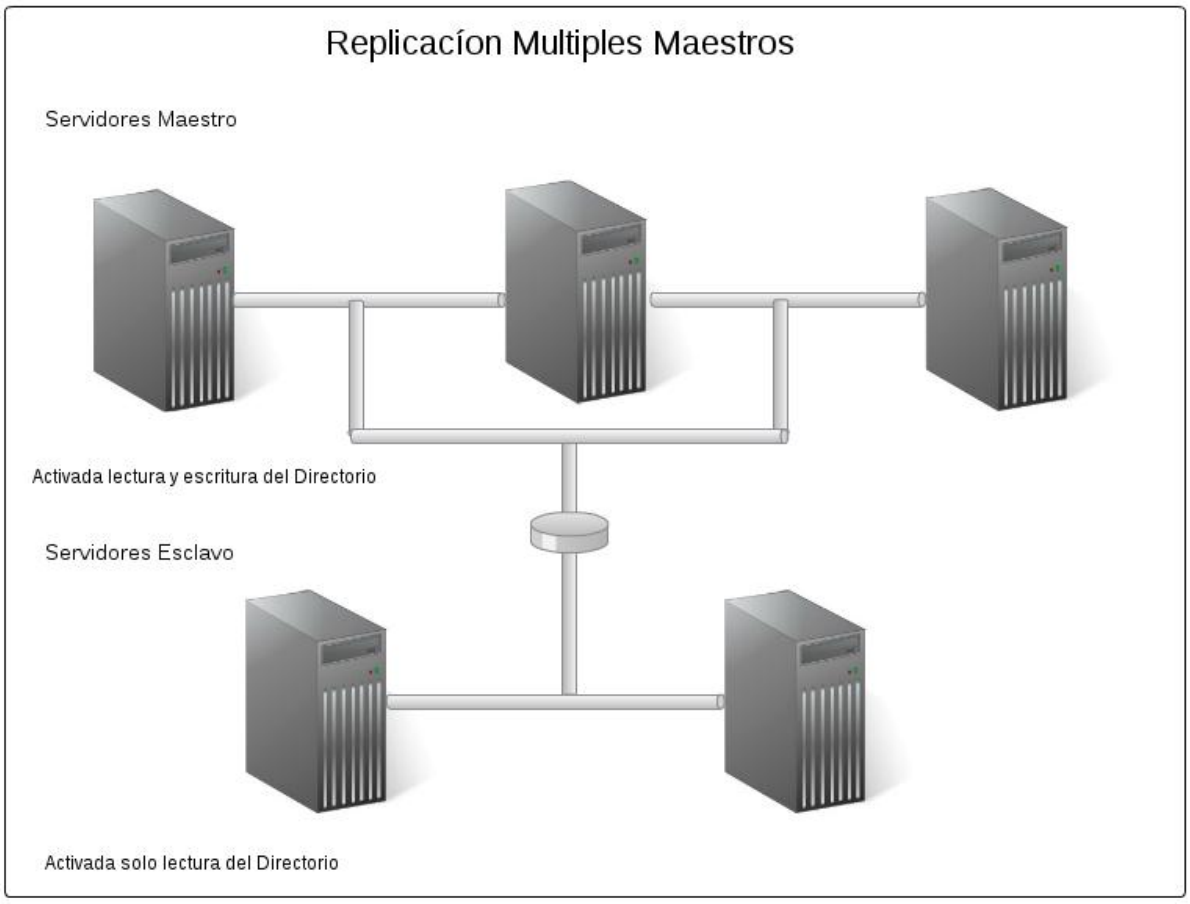
Entre las principales ventajas de utilizar este esquema de replicación está la descentralización del servicio como controlador primario de dominio permitiéndonos un mejor administración de los equipos en el domino de red local.



1.24.2. Replicación Múltiples Maestros.

En un esquema de replicación de múltiples maestros más de un servidor tienen la capacidad de leer y escribir en el Directorio Activo, es decir los clientes pueden escribir en su servidor maestro más cercano y las modificaciones serán replicadas hacia los demás servidores maestros y esclavos que se dispongan en el entorno de red.

Este esquema de replicación conocido también como Multi-master es el claro ejemplo de un esquema que permite tener una tolerancia a fallos cercano al 0% ya que nos permite realizar trabajos de mantenimiento sobre los equipos sin perdidas de servicio que sean notables para los usuarios.



La replicación con varios servidores maestros ofrece mayor fiabilidad para los clientes del Directorio Activo y los servicios que consumen información de este. Este esquema permite mantener más de un servidor LDAP principal sobre los cuales están habilitada la escritura,

además tienen soporte para políticas de resolución de conflictos de actualización. Esta política se utiliza para resolver un conflicto de actualización, lo que puede ocurrir cuando un atributo de una entrada se modifica a la vez por dos servidores maestros diferentes.

1.25. Autenticación y Autorización.

Para acceder al servicio LDAP, el cliente LDAP primero debe autenticarse con el servicio. Es decir, se debe indicar al servidor LDAP que se va a acceder a los datos para que el servidor pueda decidir lo que el cliente puede ver y hacer sobre el directorio. Si el cliente se autentica correctamente con el servidor LDAP este recibe la validación y en el servidor se habilitan los permisos a los cuales el cliente tiene acceso. Este proceso se denomina autenticación y control de acceso de usuarios en el directorio.

En OpenLdap, la autenticación se entrega en la operación de "enlace". LDAP 3 es compatible con tres tipos de autenticación, la denomina "**anónima"** cuando un cliente envía una petición al servidor LDAP sin hacer un enlace previo, la **"autenticación simple"** la que consiste en enviar al servidor LDAP el DN o nombre completo del cliente (usuario de dominio) y la contraseña en texto claro, este mecanismo tiene problemas de seguridad debido a que la contraseña puede ser leído desde la red. Para evitar exponer la contraseña de esta manera, se puede utilizar el mecanismo de autenticación simple dentro de un canal cifrado (como SSL), siempre que sean compatibles con el servidor OpenLdap, por último la conocida como "**SASL"** que viene a ser la autenticación simple pero por medio de una capa de seguridad. SASL es la autenticación sencilla y por medio de una capa de seguridad (RFC 2222). En esta se especifica un protocolo en la que se intercambian datos entre el cliente y el servidor para los fines de autenticación y establecimiento de una capa de seguridad con fines de establecer la comunicación posterior. Mediante el uso de SASL, el servidor OpenLdap puede soportar cualquier tipo de autenticación acordado entre el cliente y el servidor.

Además de autenticar a los usuarios para acceder a la información de directorio, el servidor OpenLdap puede también autenticar a los usuarios de otros servicios como Sendmail, Zimbra, vsftp, samba, etc. Esto se lleva a cabo la migración de la información específica del usuario en el servidor OpenLdap y el uso de un mecanismo llamado PAM (Pluggable Authentication Module).

1.26.Mantenimiento del directorio Activo.[35]

El mantenimiento de la información se refiere las mejores prácticas y procedimientos manejados para mantener los datos actualizados en el directorio activo. El mantenimiento de la información es una de las tareas más importantes que desempeña el administrador para proteger la integridad y la consistencia en un directorio LDAP. Es importante realizar este procedimiento ya que tiene por objetivo proporcionar acceso a información actualizada, evitando que los datos almacenados sean inexactos o considerados de mala calidad, como resultado de este proceso preservamos que la calidad de la información no se considere mala, y que los usuarios del directorio no se sientan desconformes con la información proporcionadas por este servicio y las aplicaciones que consumen información funcionen correctamente, de ahí que el mantenimiento de la información debe realizarse periódicamente.
Sin un cronograma de mantenimiento adecuado del directorio activo puede llegar a ser una de las tareas más costosas para la organización lo que técnicamente no es considerado aceptable ya que puede costar cientos de miles de dólares en tiempo del personal dedicado actualización de datos y la resolución de problemas.

1.26.1. Mantenimiento de la Información.

El propósito del mantenimiento de datos es garantizar que los mismos en el servicio de directorio tienen la calidad más alta posible. Por lo cual existen tres métodos que nos ayudaran a realizar este proceso.

1.26.1.1. Fuente de datos de origen.

Si el esquema de directorio activo está compuesto por servidores principales y servidores secundarios el proceso para validar la integridad de la información consiste en tomar un respaldo del servidor origen periódicamente y compararlo con uno de los servidores secundarios. Si la prueba de comparación es satisfactoria en hora buena, caso contrario abra que realizar el proceso de análisis de los logs del servidor principal en el cual se describen los sucesos realizados por él y sus réplicas.

[35] Ian Clatworthy. OpenLDAP Software 2.4 Administrator's Guide, The OpenLDAP Foundation, All Rights Reserved. Cuarta Edición Pág.179.

1.26.1.2. Controles al azar.

Un segundo método consiste en ejecutar controles al azar sobre los directorios distribuidos este método consiste en realizar inferencias estadísticas para informarle sobre la calidad general de los datos del directorio.

1.26.1.3. Encuestas a usuarios.

Un tercer método consiste en encuestar a los usuarios del directorio y preguntar acerca de la calidad de datos del mismo.

1.26.2. Respaldo y sistema de recuperación de desastres.

Para definir una buena estrategia de respaldos y una recuperación de información del directorio activo dependerán en gran medida del volumen de información, la frecuencia con el cual es actualizado, el tamaño que representa el respaldo, y el tiempo que este respaldo será almacenado. Por otro lado existen mecanismos de respaldos de información en los cuales el administrador del directorio se puede apoyar como son la sincronización con servidores de respaldos, almacenamiento compartido de información (SAN, NAS, etc), respaldos a medios magnéticos.

Para obtener estos respaldos del directorio se utilizaran las herramientas que proporciona el mismo servidor de directorio OpenLdap el cual nos permite obtener un respaldo del directorio en un momento indicado. La herramienta "slapcat" nos proporciona un respaldo global del directorio enviando la información a un solo archivo "LDIF" con el cual podemos regresar a un punto indicado la información del directorio. Como mencionamos anteriormente un archivo LDIF especifica un conjunto de entradas del directorio y cambios sobre las entradas del directorio las cuales nos servirán para recrear el directorio en caso de ser necesario. Para un mejor uso de la herramienta "slapcat" es recomendado que sea utilizada cuando el servicio del directorio está detenido, con esto garantizamos que la escritura sobre el mismo no pueda ser realizada mientras dura el proceso de respaldo con lo que evitaríamos tener inconsistencia con la información del directorio.

Tomando en consideración el volumen de cambio de información en el directorio estos pueden ser cada hora, día, mes, esto queda a discreción del administrador del directorio.

1.27. Controlador de Dominio Primario.

1.27.1. ¿Qué es un Controlador de Dominio?[36]

El controlador de dominio es un servicio que provee información en un dominio de red, la que puede ser utilizada por cualquier tipo de sistema operativo para la autenticación de usuarios en equipos de red o por aplicaciones desarrolladas en la organización o empresa como algunos de los servicios que proporciona. Uno de los servicios principales que facilitan los controladores de dominio es la autentificación en un entorno de red. Por medio de la autentificación podemos garantizar o denegar a un usuario el acceso a recursos compartidos. La autentificación se realiza normalmente a través del uso de contraseñas encriptadas utilizando protocolos SSL. Cada controlador de dominio usa un Security Account Manager (SAM) en Unix, o New Technology Directory Service (NTDS) en Windows Server 2003 y 2008 usados para la compartición de recursos de red y que nos permiten mantener información de nombres de usuarios y contraseñas. En resumen un servicio de controlador de dominio por medio del uso de SAM crea un repositorio centralizado de información de usuarios y contraseñas, lo cual es más eficiente que mantener en cada máquina del domino de red centenares de usuarios y contraseñas.

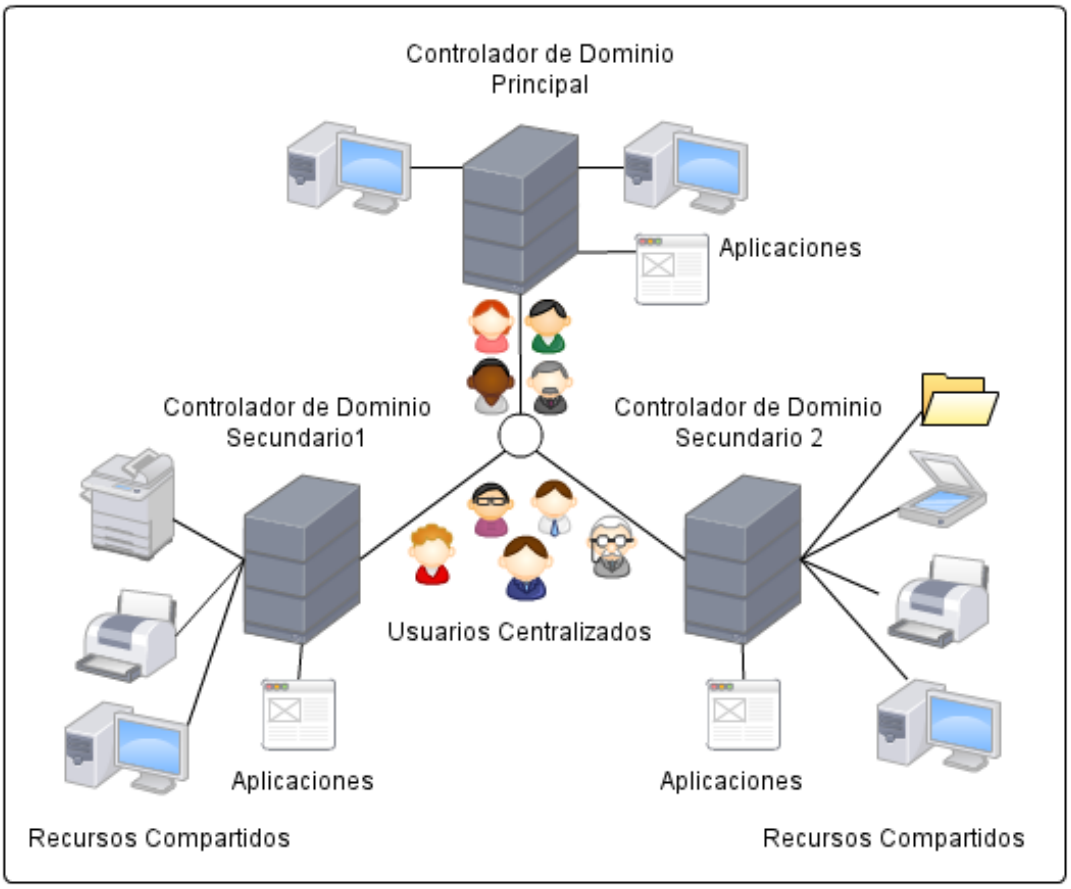
En el dominio de red, cuando un cliente solicita un acceso a los recursos compartidos de un controlador, el servidor principal verifica si ese usuario está autentificado. Si lo está, el servidor iniciara un proceso de inicio de sesión de acuerdo con los permisos de red correspondientes para ese usuario. Si no lo está, la conexión es denegada y no se procede a iniciar la sesión en el dominio de red.

Una vez que un usuario es autenticado por el controlador de dominio, una validación de autentificación será remitida, de manera que el usuario no necesitará volver a identificar para acceder a otros recursos del dominio de red hasta que el usuario cierre su sesión.

[36] John H. Terpstra and Jelmer R. Vernooij, The Official Samba 3.5.x HOWTO and Reference Guide, Prentice Hall 2007, Pag. 35

1.27.2. ¿Qué es un Dominio NetBios?[37]

Un dominio NetBIOS es un conjunto de equipos que comparten un nombre de dominio en común. Este permite acceder a las máquinas y a los usuarios por medio de una autenticación de credenciales a una sesión de dominio que permita el consumo de los recursos disponibles en la red como directorios compartidos, impresoras, etc. Estos pueden estar conformados por uno o más controladores de dominio. A pesar de que se acostumbra limitar a un dominio único un segmento de red, esto no tiene por qué ser siempre el caso, es decir pueden coexistir dos o más dominios dentro de un único segmento de red separando los recursos compartidos para ambientes como de desarrollo o de producción.

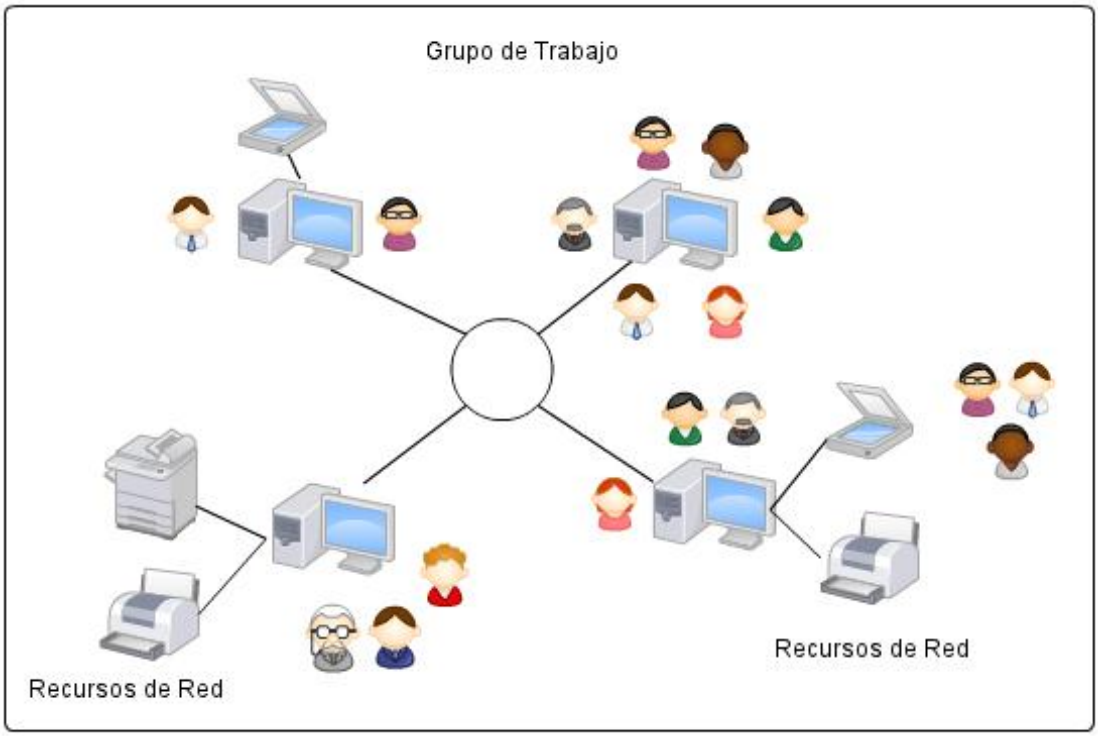


[37] Roderick W. Smith . Linux Samba Server Administration, Sybex, Primera Edicion, USA Octubre 2000 , Pag. 270

1.27.3. ¿Qué es un grupo de Trabajo?[38]

Un grupo de Trabajo es un conjunto de equipos que comparte un nombre de un grupo de trabajo dentro de una determinada red. Podríamos decir que un grupo de trabajo es un grupo de usuarios, dentro de la misma red, que trabajan en un proyecto común.

Para pertenecer a un grupo de trabajo, es necesario asignar para cada equipo el nombre del grupo al que pertenece y además asignarle a ese equipo un nombre específico que lo diferencia de los demás. La gran diferencia con un Domino de NetBios reside en que no se tiene un control centralizado de las cuentas de usuarios haciendo la administración de recursos insegura.



1.27.4. Samba y OpenLdap como controladores de Dominio.

Samba es un servidor o un cliente de código abierto que implementa protocolos de red para compartir recursos como el SMB (Server Message Block), actualmente como CIFS (Common Internet Filesystem). Esto permite a sistemas operativos Unix que actúen como servidores o

[38] Roderick W. Smith . Linux Samba Server Administration, Sybex, Primera Edicion, USA Octubre 2000 , Pag. 277

clientes en dominios de red que tengan equipos con sistemas operativos Windows o Linux, también nos permite compartir diferentes tipos de recursos: como archivos, directorios, y equipos de red como escaners impresoras, etc. Aparte de dar servicio a estos recursos la última versión de Samba3.0 también tiene la posibilidad de validar usuarios actuando como PDC "Controlador Principal de Dominio" siendo miembro de un dominio existente en la red o bien siendo el servidor maestro del dominio realizando la integración con la herramienta OpenLdap para proporcionar información de un directorio activo.

Por lo general en empresas grandes como bancos o instituciones del estado en las cuales disponen de varias agencias regionales, nacionales o internacionales donde la administración de la infraestructura se vuelve compleja y realizar la gestión de cuentas de usuario se puede convertir en una tarea de administración, se pueden acudir a utilizar esquemas de replicación de servidores de domino centralizando la información bajo una sola administración y facilitando el trabajo de los funcionarios.

Para la compartición de recursos de red de forma segura la configuración básica de Samba no es suficiente y es necesario disponer de un acceso de forma segura a través de los directorios activos que usan Secure Sockets Layer (SSL) capa de conexión segura y que unifique todo tipo de cuentas de usuario en una solo directorio de datos de acceso ligero, con el objetivo de no tener diferentes bases de datos de usuarios en Linux y en Windows las que tendríamos que administrar con herramientas por separado.

OpenLdap es una versión libre de LDAP (Lightweight Directory Access Protocol) y junto con Samba nos permite organizar de forma jerárquica todo tipo de cuentas de usuarios, realizar clasificaciones de grupos, organizar los equipos disponibles en el entorno de red, etc. OpenLdap nos permite acoplarnos a las estructuras jerárquicas de las empresas para tener un orden en la compartición de recursos e incluso para limitar el acceso a información.

Para poder realizar una mejor integración de Samba y OpenLdap y que actúen como un Controlador de Domino de Red emulando el funcionamiento del Active Directory de Microsoft es necesario realizar la instalación y configuración de utilidades extras llamadas "smbldap-tools" que nos permitirán realizar la administración en conjunto de estas dos servicios de Red de Unix.

1.28. Ventajas al uso de un Controlador de Dominio.

Entre las ventajas que existen en el uso de un controlador de dominio podemos destacar:

- La centralización de cuentas de usuarios en un directorio el cual puede ser accedido desde la red.
- La protección de información centralizada es mucho más fácil.
- Al centralizar la información el tema de respaldos se reduce a un directorio de información único.
- La recuperación de información es más rápida de realizar al disponer de esquemas de replicación de servidores principales o maestros, con servidores secundarios o esclavos.
- Es soportado el acceso a aplicaciones con las credenciales almacenadas en el directorio activo.
- Se comparte los recursos de red como impresoras, escaners, computadores.
- Permite compartir y mantener centralizada información como documentos, imágenes, etc.
- Administra perfiles de usuarios, de tal manera que no interesa en que equipo del dominio se conecta a la red, siempre mantiene sus perfiles y configuraciones.
- Gestiona y controla dominios de red complejos como entidades bancarias o gubernamentales y sus respectivas sucursales que pueden llegar a ser a nivel nacional o internacional.

La principal ventaja que brinda el servidor de Samba 3.0 es que incluye soporte para la autentificación mediante directorios LDAP, lo que se convierte en un tema imprescindible técnicamente al tener sistemas Unix y Windows comunicándose en un entorno de red sobre la cual la autenticación de un cliente permite acceder a recursos compartidos en el dominio.
La versión de samba 4.0 esta aun en etapa de desarrollo razón por la cual no será utilizada para el desarrollo de esta guía.

Resumiremos los roles que puede asumir Samba 3 como controlador de dominio integrado con OpenLdap:[39]

Roles	Soporte
Servidor de archivos	Si
Servidor de impresión	Si
Servidor DFS de Microsoft	Si
Controlador de dominio primario	Si
Controlador de dominio secundario	Si
Controlador de dominio Active Directory	No
Autentificación de clientes Windows 95/98/Me	Si
Autentificación de clientes Windows NT/2000/XP/ Windows Server/2003/2008	Si
Buscador maestro local	Si
Buscador de respaldo local	Si
Buscador maestro de dominio	Si
Servidor primario WINS	Si
Servidor secundario WINS	No

1.29. Tipos de Controladores de Dominio.[40]

1.29.1. Controlador de Dominio Principal. (PDC)

Es llamado Controlador de Dominio Principal a la combinación de dos servicios de red Samba y OpenLdap. El PDC (Primary Domain Controller) es el encargado de realizar el ingreso de información al directorio activo, por lo cual es el único que tiene activado la lectura y escritura de información. En el servidor PDC se realizan las modificaciones que serán replicadas a los demás servidores PDC o BDC en el entorno de red.

1.29.2. Controlador de Dominio Secundario.[41]

Es llamado Controlador de Dominio Secundario a la combinación de dos servicios de red que son réplica del servidor Samba y OpenLdap del Controlador de Dominio Principal. El objetivo

[39] Gerald Carter, Jay Ts, and Robert Eckstein, Using Samba, Tercera Edicion, Oreally 2007, Pag. 28
[40] John H. Terpstra and Jelmer R. Vernooij, The Official Samba 3.5.x HOWTO and Reference Guide, Prentice Hall 2007, Pag. 166
[41] John H. Terpstra and Jelmer R. Vernooij, The Official Samba 3.5.x HOWTO and Reference Guide, Prentice Hall 2007, Pag. 166

de tener un Servidor BDC (Backup Domain Controller) es proporcionar información solo de lectura y no de escritura sobre el servidor de directorio principal, descentralizar los requerimientos hacia el servidor PDC como son la autentificación de equipos o aplicaciones que consuman información del Directorio.

La configuración de servidores BDC en un entorno de red también son considerados como un método para mantener una tolerancia mínima a fallos.

1.30. Administración de Usuarios y Grupos[42]

Para la administración de cuentas de Usuarios y de Grupos dentro del esquema SAMBA-LDAP utilizaremos el conjunto herramientas de integración para estas que se encuentran agrupadas en un paquete de instalación conocida como smbldap-tools. Estas herramientas están disponibles desde la versión de Samba 3.0. Las herramientas que provee el paquete smbldap-tools, son un conjunto de scripts que se ejecutan sobre las herramientas del sistema operativo para las tareas de administración de usuarios y de grupos de SAMBA-LDAP que permiten la creación, eliminación, modificación y políticas de seguridad para usuarios y grupos.

Adicionalmente, incorporan scripts para facilitar la migración de servidores PDC de Windows NT 4.0 a servidores PDC Samba-LDAP en caso de requerirlo. Estas son: smbldap-populate, smbldap-migrate-groups y smbldap-migrate-accounts

1.31. Servicios que implementa el uso del servidor PDC-SAMBA[43]

El servicio de Samba contiene muchos demonios que prestan distintos servicios que tienen propósitos relacionados para realizar la integración de las cuentas de usuarios SAMBA-LDAP con la compartición de recursos en la red. Podemos realizar un resumen de los demonios más utilizados para la administración de cuentas en un PDC.

- ***Nmbd***

El demonio nmbd es un simple servidor de nombres que suministra la funcionalidad de

[42] John H. Terpstra and Jelmer R. Vernooij, The Official Samba 3.5.x HOWTO and Reference Guide, Prentice Hall 2007, Pag. 39

[43] Gerald Carter, Jay Ts, and Robert Eckstein, Using Samba, Tercera Edicion, Oreally 2007, Pag.30

WINS (Windows Internet Name Service). Este demonio espera peticiones del servidor de nombres y proporciona la dirección IP apropiada cuando se le requiere. También provee una lista de búsqueda para el entorno de red y participa en la elección de búsqueda.

- ***Smbd***

  El demonio smbd maneja los recursos compartidos entre el servidor Samba y sus clientes. Provee los servicios de servidor de archivos, impresión y búsqueda a los clientes SMB, maneja todas las notificaciones entre el servidor Samba y la red de clientes. Es también el responsable de la autentificación de usuarios, bloqueo de recursos y compartición de datos a través del protocolo SMB.

  A partir de la versión Samba2.2 se añadió otro nuevo demonio llamado el Winbind.

- ***Winbind***

  Este demonio se utiliza junto con el servicio de nombres para obtener la información de los usuarios y grupos desde un servidor Windows NT y permitir a Samba autorizar a los usuarios dentro de un servidor Windows NT/2000.

Samba posee además un conjunto de pequeñas herramientas para consola, a continuación se mencionan las más significativas:

- ***Findsmb***

  Este programa realiza búsquedas de ordenadores en la red local que respondan al protocolo SMB e imprime información sobre los mismos.

- ***Make_smbcodepage***

  Este programa es utilizado cuando se trabaja con la característica de internacionalización de Samba para informarle sobre cómo convertir entre mayúsculas y minúsculas en los distintos conjuntos de caracteres.

- ***Net***

  Es incorporado en las versiones más recientes de samba es distribuido con Samba 3.0 y es utilizado para realizar una administración remota de los servidores.

- ***Nmblookup***

  Este programa realiza búsquedas de nombres sobre NBT para encontrar direcciones IP de ordenadores cuando se da su nombre de máquina.

- ***Pdbedit***

  Por medio de esta aplicación se pude administrar las cuentas de usuarios, es usada para establecer políticas de seguridad de los usuarios.

- ***Smbclient***

  Un cliente Unix similar a un cliente ftp, que se puede utilizar para conectarse a los recursos compartidos SMB y operar con ellos.

- ***Smbgroupedit***

  Una orden que se puede utilizar para definir mapeos entre los grupos de Windows NT y los de Unix. Esta es una funcionalidad nueva en Samba 3.0.

- ***Smbpasswd***

  Un programa que permite a un administrador cambiar la clave utilizada por Samba.

- ***Smbstatus***

  Un programa que reporta las conexiones de red realizadas a los recursos compartidos en el servidor Samba actualmente.

- ***Testprns***

  Un programa que comprueba el archivo de configuración de Samba.

1.32. Alta Disponibilidad

1.32.1. ¿Qué es la Alta Disponibilidad? [44] [45]

El Concepto de Alta Disponibilidad hace referencia a la capacidad de proporcionar continuidad operacional a un servicio, sistema o aplicación con un mínimo de interrupciones durante un porcentaje de tiempo determinado. La disponibilidad se mide en intervalos de tiempo que pueden ser minutos u horas dependiendo del período de medición dado y de la naturaleza del servicio. La manera de calcularla es de acuerdo a la siguiente formula:

Altdisp= MTBF/(MTBF + MTTR)

Dónde:

- **Altdips,** representa la disponibilidad general del servicio dentro del espacio de tiempo que se mide la accesibilidad.
- **MTBF**-Mean Time Between Failure, representa el tiempo promedio entre fallas
- **MTTR**-Mean Time To Repair, representa el tiempo medio para la reparación una vez ocurrida la falla y detectada.

Mantener la Alta Disponibilidad de un servicio o aplicativo consiste en que estos se mantengan operativos durante las 24 horas al día, 7 días a la semana, los 365 días del año, lo que representa para los administradores en mantener un plan estratégico para la continuidad del servicio o negocio. Se debe considerar planes para la recuperación de desastres y el tiempo que estos representen.

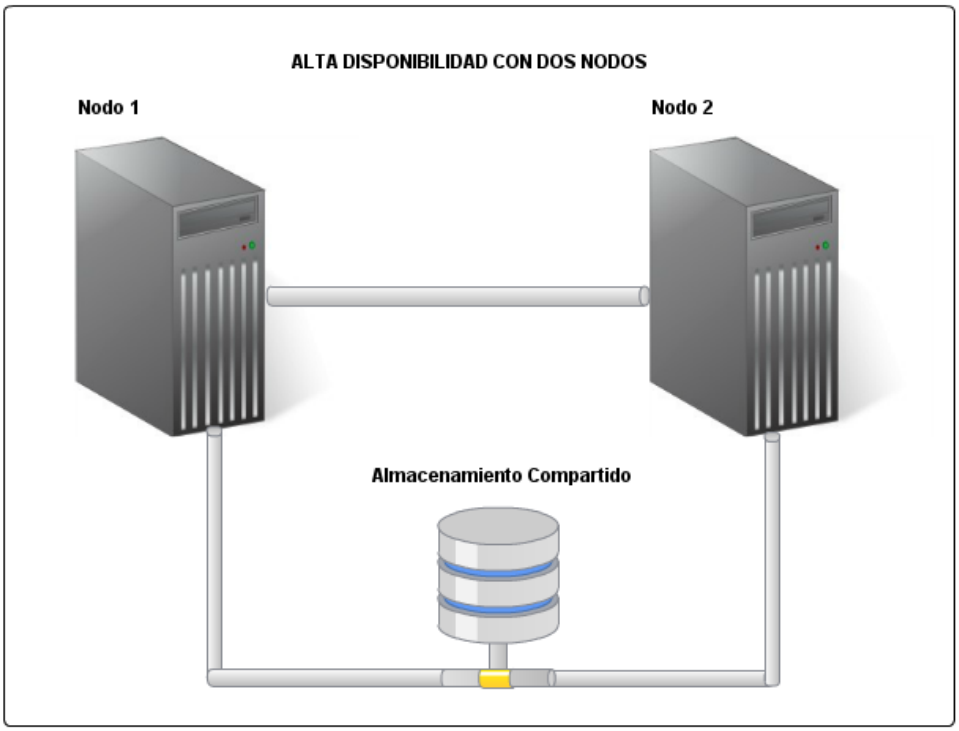
Comúnmente cuando un servicio o aplicativo falla se debe a dos razones una por un fallo de hardware y la otra por un fallo humano que normalmente es debido a un error en la administración del servicio o aplicativo.

Los sistemas de alta disponibilidad se basan en la replicación de los servicios o aplicativos sobre varias plataformas de hardware permitiendo reducir el porcentaje de tiempo de inactividad, lo que es conocido como implementación de sistemas tolerantes a fallos, al mantener una alta disponibilidad a nivel de hardware hablamos de un clúster de alta

[44] Dilip Ranade. Shared Data Clusters Scalable, Manageable, and Highly Available Systems. Wiley Publishing, Inc. 2002 Pag. 89

[45] Chris Oggerino. High Availability Network Fundamentals. Cisco Press. April 2001. Pag. 11

disponibilidad. Este tipo de configuración eleva los costos de infraestructura en los centros de datos pero reduce los tiempos de inactividad de un servicio o aplicativo permitiendo brindar un servicio continuo durante todo un periodo de tiempo que generalmente se lo conoce como 24x7x365.



1.32.2. Factores que afectan la alta disponibilidad.[46]

Existen varias consideraciones que se necesitan para la implementación de un sistema de alta disponibilidad y que muchas de las veces no se toman en cuenta. La mayoría de diseñadores de red solo consideran el factor de hardware como un único punto de fallo sobre la red, sin embargo se deben considerar otros como ejemplo:

- ***El software.***

  La parte más difícil de considerar en el cálculo de la disponibilidad del software es determinar qué MTBF se debe usar. Muchos métodos están disponibles para el cálculo

[46] Chris Oggerino. High Availability Network Fundamentals. Cisco Press. April 2001. Pag 43

de la fiabilidad del software, y en su mayoría son muy difíciles de realizar o no son muy precisos. La mejor de las maneras más sencillas de obtener un MTBF precisa para el software es hacer mediciones en el transcurso de actividades en día a día. Las empresas que desarrollan software deben realizar estas mediciones en conjunto con sus clientes y proporcionar los resultados de estos. De esta forma sus clientes podrán disponer de un mecanismo para la realización de los cálculos de disponibilidad con el aporte del software incluido.

- ***Consideraciones del entorno físico sobre los equipos.***

  En algunos sistemas de red extensos puede ser difícil realizar el cálculo de tiempo de inactividad y quizás por ello no se lo realiza pero este es un gran error que cometen los administradores. Para instituciones bancarias es de gran importancia mantener sitios alternos donde se pueda levantar la infraestructura de red para brindar nuevamente su servicios por lo cual es importante tener en cuenta el ambiente donde están los centros de información. Estas consideraciones son cruciales al momento de definir físicamente un centro de datos y entre ellas debemos tener en cuenta que no deben estar en subsuelos ya que pueden ser afectadas por inundaciones. La ventilación de un centro de datos debe ser una de las mayores consideraciones debido a que el polvo puede dañar los sistemas mecánicos de los centros de almacenamiento de información La continuidad en la electricidad sin hacerla de menos a las anteriores debe ser considerada al momento del diseño del centro de información debido que la mayoría de fallos en los sistemas de red son presentadas por fallas en la electricidad.

- ***Operaciones sobre la red y errores humanos.***

  Una de las consideraciones más difíciles de determinar para los sistemas altamente disponibles son los errores humanos. Este tipo de fallas no es difícil de corregir y evitarlas. La dificultad surge cuando tratamos de predecir estos errores con antelación. El error humano normalmente se produce cuando los procesos de operaciones estándar permiten que estos sucedan. La definición de procesos en una organización reduce los errores humanos lo que constituye uno de los pilares en la administración de sistemas

de alta disponibilidad y el cual está basado en un simple algoritmo constituido por 4 fases claves los cuales son:

- ***Predicción.***

  Se considera como la primera fase en la cual es indispensable determinar los procesos que se realizan para la administración de los sistemas altamente disponibles.

- ***Medición.***

  En la Segunda fase se debe establecer el tiempo de operación de los servicios involucrados este incluye el tiempo de actividad y de inactividad.

- ***Análisis.***

  En la tercera fase de este ciclo se debe realizar informes sobre los resultados obtenidos en la fase anterior para mejorar los procesos establecidos.

- ***Gestión de Cambios.***

  En la fase final sobre la cual se realizan cambios sobre los procesos definidos mejorándolos y cerrando el ciclo de procesos en la administración de los sistemas que se estarían en alta disponibilidad.

- ***El mismo diseño de la red.***

  El diseño de la red influye en la determinación de tiempos de inactividad de los sistemas altamente disponibles debido a los protocolos de comunicación que estos definen. La conectividad entre los equipos que se encuentran en este esquema de configuración de alta disponibilidad debe ser permanente. Por ello es importante definir segmentos de red que faciliten el tráfico de información sobre la misma.

Tomando en cuenta cada uno de estos factores mencionados al realizar la planificación de un entorno de alta disponibilidad la capacidad para determinar un valor de continuidad operacional será mucho más precisa que solo considerar como (SPF) al hardware destinado

para soportar este entorno.

A pesar de que el hardware nos proporciona un valor fácil para la estimación global del tiempo en que el servicio no estará disponible, no sucede lo mismo con el software ya que este puede ser medido dependiendo de la subjetividad con que se maneje la misma.

1.32.3. ¿Qué es un único punto de fallo?[47]

Es el concepto relacionado con la falla de un equipo o un servicio configurados sobre una infraestructura informática que no disponga de un esquema de respaldo y que el en caso de presentar fallas en su operación este genere problemas significativos en la continuidad del negocio de la empresa u organización. Para mantener una infraestructura informática segura se debe de evitar tener SPOF (single point of failure), puntos únicos de falla sobre la misma.

1.33. Ventajas de Usar alta disponibilidad.

La implementación de sistemas altamente disponibles sobre los servicios o aplicativos nos permite:

- Mejorar la disponibilidad del sistema al proporcionar un servicio continuo aun durante la falla de hardware o software.
- Incrementar la confiabilidad de operación del negocio.
- Eliminar las fallas del sistema por errores con el hardware.
- Disponibilidad y acceso a los datos ante la posibilidad de fallo de uno de los nodos.
- Mejorar la escalabilidad de procesamiento al permitir agregar nodos extras a la configuración del clúster.
- Permite realizar un balanceo de carga de los servicios o recursos entre los nodos que conforman el clúster.

[47] Dilip Ranade. Shared Data Clusters Scalable, Manageable, and Highly Available Systems. Wiley Publishing, Inc. 2002 Pag 136

1.34. Recursos de un Sistema de Alta Disponibilidad.[48]

Para el funcionamiento de los llamados sistemas de alta disponibilidad se necesitan de varios componentes que se describirán a continuación.

1.34.1. Nodos.

Los nodos en un sistema de alta disponibilidad se consideran a los equipos encargados de realizar el procesamiento de información que es compartida entre los miembros del sistema de alta disponibilidad.

1.34.2. Sistemas de Almacenamiento.

Los sistemas de almacenamiento en los sistemas de alta disponibilidad son los medios sobre los cuales la información es almacenada y compartida. Es importante mantener un medio de almacenamiento eficiente ya que de este dependerá el rendimiento del acceso a la información en los sistemas de alta disponibilidad.

1.34.3. Sistema Operativo.

El sistema operativo que se utilizara en un sistema de alta disponibilidad debe ser multiproceso y multiusuario. Existen distribuciones específicas que se componen de un sistema operativo y del software que permite realizar la configuración de un entorno de alta disponibilidad, como lo es Red Hat que será utilizado para el desarrollo de esta guía metodológica.

1.34.4. Conexiones de red.

La interconexión que se maneja entre los nodos es muy importante dentro de la arquitectura de un sistema de alta disponibilidad y es considerada como un elemento crítico dentro de los sistemas de alta disponibilidad.

La tecnología de conexión puede ser desde la más barata y extendida ethernet hasta las más caras y avanzadas como Myrinet o Infiniband. Estas últimas cuentan con mayor ancho de

[48] Phil Lewis, A high-availability cluster for Linux. Internet. http://linuxjournal.com/issue64/3247.html.(10/09/2013)

banda y menor latencia.

1.34.5. Middleware.

El middleware es una pieza de software que se sitúa entre el sistema operativo y las aplicaciones con el fin de proveer:

- ***Abstracción del hardware*:** En la cual los usuarios ven el al sistema de alta disponibilidad como un único ordenador con el que interactúan, desentendiéndose de la arquitectura subyacente.
- ***Herramientas de gestión del sistema*:** En la cual se puede realizar la migración de procesos, balanceo de carga, tolerancia a fallos, etc.
- ***Escalabilidad*:** En la cual se realiza la detección e incorporación automática de nuevos nodos al sistema de alta disponibilidad.

1.34.6. Aplicaciones.

Las aplicaciones vienen a ser el motivo por el cual se implementan estos sistemas de alta disponibilidad con el principal objetivo de siempre permitir un acceso a la información que estos brinden a los usuarios.

1.35. Redundancia en un entorno de Alta Disponibilidad.

Definiremos la redundancia como el empleo de información, recursos o tiempo adicionales, por encima de los estrictamente necesarios para el correcto funcionamiento de un sistema de alta disponibilidad.

1.35.1. Redundancia hardware o física.

Consiste en incorporar hardware adicional, normalmente con el fin de detectar fallos o conseguir la tolerancia ante los mismos.

1.35.2. Redundancia software.

Consiste en añadir en los programas líneas de código adicionales para evitar errores. Este código suplementario puede tener diferentes funciones, tales como evitar que los datos se salgan de rango, prevenir errores aritméticos, etc.

1.35.3. Redundancia informacional.

Este tipo de redundancia implica el manejo de información suplementaria con el fin de detectar o corregir errores potenciales.

1.35.4. Redundancia temporal.

Consiste en emplear tiempo adicional de proceso para detectar posibles fallos, o en su caso, corregirlos. Esto puede suponer, por ejemplo, la repetición de cálculos por diferentes métodos.
Estos tipos de redundancia no son excluyentes y en muchas ocasiones funcionan en conjunto por ejemplo se pude mencionar que la redundancia software implica redundancia temporal salvo si se emplea un procesador suplementario para ejecutar las instrucciones adicionales en cuyo caso existirá redundancia hardware, otro ejemplo seria referente a la redundancia informacional puede hacer necesario un incremento de memoria para almacenar la información adicional en la que se presentaría redundancia hardware.

1.36. Servicio de datos en un entorno de Alta Disponibilidad.

Se denomina servicio de datos a un determinado servicio o aplicación que se configure en el entorno de alta disponibilidad y los recursos necesarios para que el servicio sea puesto en producción para proveer información. En otros entornos de alta disponibilidad se denominan *logical host o software packages* a la unión de servicio de datos y grupo de recursos asociados a este.
Estos grupos de recursos han de implementar mecanismos necesarios, para que sean completamente flexibles entre nodos del sistema de alta disponibilidad, es decir puedan ser suplantados o cambiados físicamente entre otros nodos sin que el servicio o aplicación sea afectada.

1.37. Tipos de Alta Disponibilidad.[49]

1.37.1. Alta disponibilidad a nivel de hardware.

El software de alta disponibilidad configurado en cada uno de los nodos del clúster monitorea el estado de operatividad de estos, en caso de producirse un fallo en el hardware en uno de estos nodos el software de alta disponibilidad es capaz de arrancar automáticamente los servicios configurados en otro nodo del clúster. Y cuando el nodo que ha reportado con inconvenientes de hardware es restablecido a su normal operación los servicios son nuevamente migrados a este. Esta capacidad de recuperación automática permite mantener un entorno de alta disponibilidad a nivel de hardware sobre los nodos configurados que actúan en el clúster.

1.37.2. Alta disponibilidad a nivel de aplicación.

El software de alta disponibilidad configurado en cada uno de los nodos del clúster está en constante monitoreo de los servicios. El software de alta disponibilidad es capaz de identificar y dar de baja al nodo del clúster que presenta fallas y proceder con el proceso de arrancar automáticamente el o los servicios que han presentado inconvenientes en cualquiera de los otros nodos del clúster. Cuando el nodo que ha presentado anomalías sobre un servicio es recuperado a su estado original, los servicios son nuevamente migrados a este nodo y se procede con la restauración del clúster. Esta capacidad de recuperación automática de servicios nos garantiza la integridad de la información que por lo general se encuentra compartida en un medio de almacenamiento independiente de cada nodo del clúster, evitando pérdida de datos y manteniendo una integridad sobre la información que administra.

1.38. Configuraciones de Alta Disponibilidad.

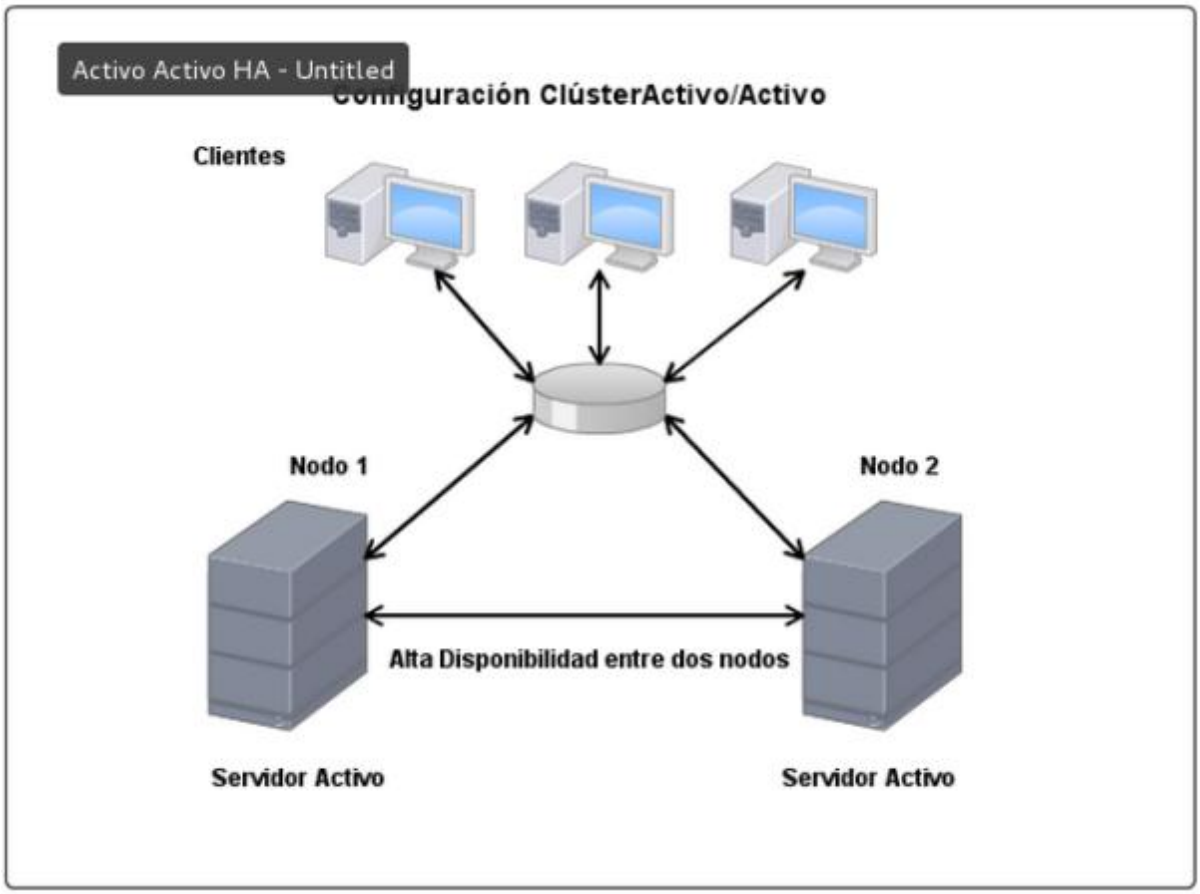
1.38.1. Configuración Activo/Activo.

En una configuración activo/activo, todos los servidores del clúster pueden ejecutar los mismos recursos simultáneamente. Es decir, los servidores poseen los mismos recursos y pueden acceder a estos independientemente de los otros servidores del clúster. Si un nodo del

[49]Universidad Nacional Autónoma de México "Que es un clúster" Revista Digital Universitaria Numero 2 junio 2003 http://www.revista.unam.mx/vol.4/num2/art3/cluster.htm#3

sistema falla y deja de estar disponible sus recursos siguen estando accesibles a través de los otros servidores del clúster.

La ventaja principal de esta configuración es que los servidores en el clúster son más eficientes ya que pueden trabajar todos a la vez. Los clientes acceden al servicio o recursos de forma transparente y no tienen conocimiento de la existencia de varios servidores formando un clúster.



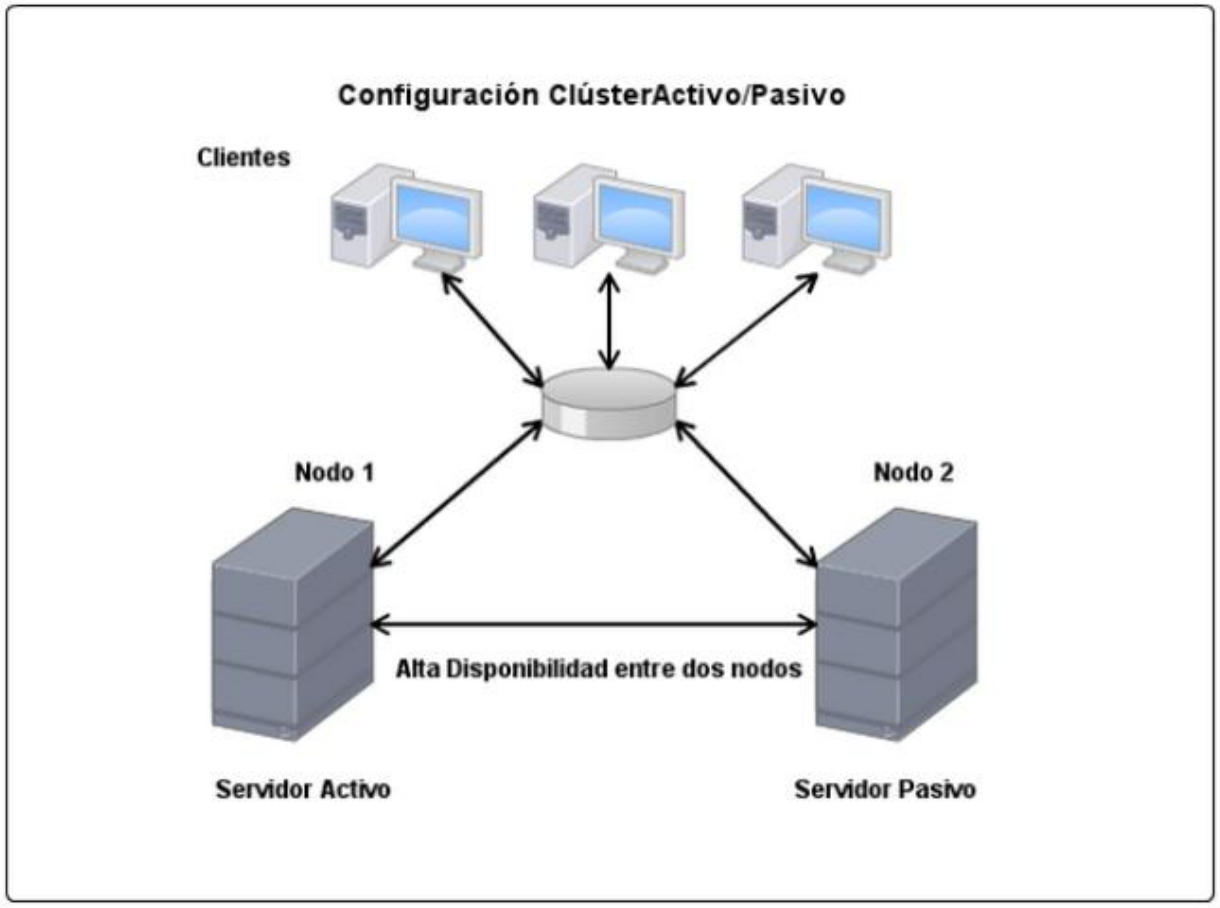
1.38.2. Configuración Activo/Pasivo.

En este tipo de clúster solamente hay un nodo que da servicio, es decir que hay un servidor que posee los recursos del clúster y otros servidores que son capaces de acceder a esos recursos, pero no los activan hasta que el propietario de los recursos ya no esté disponible.

Las ventajas de la configuración activo/pasivo son que no hay degradación de servicio y que los servicios solo se reinician cuando el servidor activo deja de responder. Sin embargo, una desventaja de

esta configuración es que los servidores pasivos no proporcionan ningún tipo de recurso mientras están en espera, haciendo que la solución sea menos eficiente que el clúster de tipo activo/activo.

Otra desventaja es que los sistemas tardan un tiempo en migrar los recursos (failover) al nodo en espera.



1.39. Integridad de datos y recuperación de servicio

1.39.1. Caracterización de los fallos.

Los fallos pueden caracterizarse atendiendo a varios criterios: causa, naturaleza, duración, extensión y variabilidad.

1.39.1.1. Causas.

Las causas para que se produzcan fallos pueden ser desde especificaciones incorrectas en el momento del diseño de la solución informática, fallos en el proceso de implementación, defectos en los componentes con los cuales se realizara la solución.

1.39.1.2. Naturaleza.

La naturaleza identifica la parte del sistema software o hardware que provoca el fallo en el sistema.

1.39.1.3. Duración.

Pueden ser de tres tipos:

- ***Permanentes*** que se caracterizan por continuar indefinidamente en el tiempo si no se toma alguna acción correctora.
- ***Intermitentes*** que aparecen, desaparecen y pueden reaparecer, de forma repetida y aleatoria.
- ***Transitorios*** que aparecen únicamente durante breves instantes coincidiendo con alguna circunstancia, tal como puede ser el encendido o alguna perturbación externa.

1.39.1.4. Extensión.

La extensión de un fallo indica si sólo afecta a un punto localizado o si afecta a la globalidad del hardware, del software o de ambos.

1.39.1.5. Variabilidad.

De acuerdo a la variabilidad los fallos pueden ser:

- ***Determinados***. Si su estado no cambia con el tiempo, incluso aunque cambie la entrada u otras condiciones,
- ***Indeterminados.*** Cuyo estado puede cambiar cuando varíen algunas de las condiciones.

1.39.2. Tolerancia a errores o fallos.

Con la creciente tecnología algunas de las aplicaciones o servicios han llegado a convertirse en críticas para el funcionamiento de una empresa u organización como por ejemplo el correo electrónico o el acceso a recursos de red, por lo cual la implementación de sistemas de alta disponibilidad son esenciales para este tipo de servicios y así garantizar la disponibilidad del servicio.

Definiremos conceptos fundamentales en el ámbito de la tolerancia a fallos:

- ***¿Qué es un Fallo?***

  Se llamara fallo a cualquier defecto, físico o lógico, en cualquier componente, hardware o software de un sistema. Diremos que un fallo se enmarca en el universo físico. Como puede ser un daño en la red, un daño de una memoria de un equipo, o la pérdida de un disco.

- ***¿Qué es un Error?***

  Un error vendría a ser la consecuencia de un fallo desde el punto de vista de la información. Los errores se enmarcan dentro del llamado universo informacional. Como por ejemplo errores en el contenido de la información de un usuario en el directorio como presentar información incompleta o no poder visualizar toda la información relacionada con este objeto.

- ***¿Qué es una Avería?***

  Una avería seria el producto de un mal funcionamiento del sistema desde el punto de vista externo. Es decir, si las consecuencias del fallo trascienden al exterior del sistema, diremos que se ha producido una avería. Las averías se producen en el universo externo o universo del usuario. Ejemplo al fallar el servicio de directorio activo no permitirá el acceso a aplicaciones o no permitirá acceder a recursos en la red.

- ***¿Qué es la latencia de un fallo?***

  La latencia de un fallo vendría a ser el tiempo que transcurre desde que se produce un fallo hasta que se manifiesta el error.

- ***¿Qué es la latencia de un error?***

  La latencia de un error es el tiempo transcurrido entre la aparición de un error y la manifestación de ese error en el exterior del sistema.

1.39.3. Puntos de fallo[50]

1.39.3.1. Failover.

Es el término usado para identificar que un nodo del clúster debe asumir la responsabilidad de otro nodo que ha presentado algún tipo anomalía. Una situación de failover es soportada cuando se dispone de más de un nodo en el clúster. Si sólo queda un nodo en el clúster tras los fallos de los demás, estaremos cayendo en malas prácticas para la administración de una infraestructura llegando a tener un SPOF hasta que el administrador del sistema realice las tareas respectivas para la restauración del clúster.

1.39.3.2. Takeover.

Es un failover automático que se produce cuando un nodo nota un fallo en el servicio de datos. Para ello debe haber cierta monitorización con respecto al servicio de datos. El nodo que se declara fallido es forzado a ceder el servicio y recursos, o simplemente eliminado de la configuración del clúster hasta que este sea validado y puesto en operación nuevamente por el administrador.

1.39.3.3. Switchover o Giveaway.

Es un failover manual, consiste en ceder los recursos de un servicio de datos y este mismo, a otro nodo del clúster, mientras se realizan ciertas tareas administrativas.
A este procedimiento se le denomina “Node outage”.

[50] http://techthoughts.typepad.com/managing_computers/2007/10/split-brain-quo.html

1.39.3.4. Fencing.

En los clusters HA existe una situación donde un nodo deja de funcionar correctamente pero todavía sigue levantado, accediendo a ciertos recursos y respondiendo peticiones. Para evitar que el nodo corrompa recursos o responda con peticiones, los clústeres lo solucionan utilizando una técnica llamada Fencing.

1.39.3.5. Split-Brain.

Escenario en el que los nodos del clúster se dividen en dos o más grupos que no saben el uno del otro (ya sea a través de un fallo de software o hardware), provocando que más de un servidor o aplicación pertenecientes a un mismo clúster intenten acceder a los mismos recursos, lo que puede causar daños a dichos recursos. Este escenario ocurre cuando cada servidor en el clúster cree que los otros servidores han fallado e intenta activar y utilizar dichos recursos.

1.39.3.6. Quorum.

Es el nombre que se le da al mecanismo cuyo objetivo es ayudar a resolver el problema SplitBrain. La solución que plantea quorum es la de no seleccionar más de una "partición del clúster", cuando falla la comunicación, es decir, que sólo una partición del clúster ofrezca los servicios.

1.39.4. Copias de seguridad.

La configuración de una arquitectura redundante asegura la disponibilidad de los datos del sistema pero no los protege de los errores cometidos por los usuarios ni de desastres naturales, tales como incendios, inundaciones o incluso terremotos.

Por lo tanto, es necesario prever mecanismos de copia de seguridad (lo ideal es que sean remotos) para garantizar la continuidad de los datos.

Además, un mecanismo de copia de seguridad también se puede utilizar para almacenar archivos, es decir, para guardar datos en un estado que corresponda a una cierta fecha.

1.40. Niveles de disponibilidad del sistema.[51]

Las herramientas de alta disponibilidad deben permitirnos disponer de nuestros equipos funcionando 24 horas al día, 7 días a la semana, ofreciéndonos la seguridad de que bajo cualquier supuesto, nuestro sistema de producción estará disponible casi inmediatamente ante cualquier imprevisto.

Se debe de diferenciar dos tipos de interrupciones en los sistemas de alta disponibilidad así como también los niveles de disponibilidad.

1.40.1. Las interrupciones previstas.

Las que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.

1.40.2. Las interrupciones imprevistas.

Las que suceden por acontecimientos imprevistos como un fallas en la corriente eléctrica, en hardware, en la configuración del software, problemas de seguridad, desastres naturales, virus.

1.40.3. Sistemas de disponibilidad base.

El sistema está listo para el uso inmediato, pero experimentará tanto interrupciones planificadas como no planificadas.

1.40.4. Sistemas de disponibilidad alta.

Incluyen tecnologías para reducir drásticamente el número y la duración de interrupciones imprevistas. Todavía existen interrupciones planificadas, pero los servidores incluyen herramientas que reducen su impacto.

1.40.5. Entornos de operaciones continuas.

Utilizan tecnologías especiales para asegurarse de que no hay interrupciones planificadas para backups, actualizaciones, u otras tareas de mantenimiento que obliguen a no tener el sistema disponible.

[51] Dossier. “Alta Disponibilidad http”. Internet. http://www.recursos-as400.com/dossier/ad/02.shtml

1.40.6. Sistemas de la disponibilidad continúa.

Van un paso más lejos para asegurarse de que no habrán interrupciones previstas o imprevistas que interrumpan los sistemas. Para alcanzar este nivel de la disponibilidad, las compañías deben utilizar servidores duales o los clústeres de servidores redundantes donde un servidor asume el control automáticamente si el otro servidor cae.

1.40.7. Sistemas de tolerancia al desastre.

Requieren de sistemas que permanezcan físicamente en puntos distantes y que tengan permanente sincronización entre ellos para asumir el control en cuanto pueda producirse una interrupción provocada por un desastre.

1.41. Glosarios de Términos.

ITU-T – Unit of International Telecommunication. Union international de telecomunicaciones.

PDC Primary Domain Controler – Controlador de Dominio Principal

BDC Backup Domain Controler – Controlador de Dominio Secundario

SAM – Security Account Manager

NTDS NT Directory Servers – New Technology Servers

WINDOWS NT – Windows New Technology

Kerberos – Es un protocolo de autenticación

Nodos o sistemas.

Los servidores que integran un clúster, vienen a ser los equipos físicos o virtuales.

Clúster.

El servicio de clúster consiste en la colección de componentes de hardware y software que efectúa actividades específicas en un sistema de red de forma conjunta.

Recursos. Los recursos son los componentes de hardware y software dentro del clúster que son administrados por el servicio de clúster.

Logical host o Software Packages. Se llama a la unión de servicio de datos y grupo de recursos asociados a un entorno de alta disponibilidad.

WINS (Windows Internet Name Service)

Es un servidor de nombres de para NetBIOS, que se encarga de mantener una tabla con la correspondencia entre direcciones IP y nombres NetBIOS, de los equipos que conforman la red local. Esta lista permite localizar rápidamente a otro equipo dentro de la red. Al utilizar un servidor WINS se evita el realizar búsquedas innecesarias a través de difusión (broadcast) reduciendo sustancialmente el tráfico de red.

SMB. (Server Message Block)

Los sistemas operativos Microsoft Windows y OS/2 utilizan SMB para compartir por red archivos e impresoras y para realizar tareas asociadas. Gracias al soporte de este protocolo, Samba permite a las máquinas Unix comunicarse con el mismo protocolo de red que Microsoft Windows y aparecer como otro sistema Windows en la red (desde la perspectiva de un cliente Windows).

Kerberos.

Es un protocolo de autenticación de redes creado por el MIT que permite realizar la autenticación de cuentas de usuarios de manera segura.

Servidor DFS de Microsoft.

El Sistema de Archivos Distribuido (DFS - Distributed File System) permite facilitar a los usuarios el acceso y la administración de archivos que se encuentran distribuidos a través de la red. Con DFS, se puede hacer que parezca que los archivos distribuidos por múltiples servidores residen en un sitio de la red a ojos de los usuarios. Los usuarios ya no tienen que saber y especificar la ubicación física real de los archivos para tener acceso a éstos.

SAM Security Account Manager.

Administrador de cuentas de seguridad (SAM) se la considera como una base de datos almacenada en un archivo del registro en Windows NT, Windows 2000, y versiones posteriores de Microsoft Windows. Almacena las contraseñas de los usuarios en un formato con hash (seguro, cifrado).

NTDS New Technology Directory Service.

Administrador de cuentas de seguridad en Windows NT, Windows 2000, y versiones posteriores de Microsoft Windows. Almacena la información de los usuarios en un directorio con sus credenciales de autenticidad.

CAPÍTULO 2

2. Desarrollo de la Guía metodológica para la Implementación de un Protocolo Ligero de Acceso a Directorios con un Controlador de Dominio Principal en un entorno de Alta disponibilidad.

2.1 Instalación y configuración del sistema operativo.

Para la instalación y configuración del Sistema Operativo en el desarrollo de esta guía metodológica se ha optado por la última versión comercial de Red Hat Enterprise Linux 6.5 x86_64 o conocido como (RHEL6.5_x86_64).

Para la instalación del Sistema Operativo RHEL6.5 se debe considerar la plataforma sobre la cual se realizará la instalación y configuración del entorno de alta disponibilidad de los servicios del OpenLdap y Samba, en este caso específico se utilizará la plataforma de virtualización conocida como Kernel-based Virtual Machine (K.V.M.) la cual puede emular un entorno virtual muy similar un centro de datos físico real.

Para el desarrollo de esta guía metodológica se procederá con la configuración de los siguientes servidores.

Equipos Virtuales para el entorno de Alta Disponibilidad OpenLdap – Samba.

No	Nombre	Descripción
1	Clster-manager.	Consola de administración del entorno de Alta Disponibilidad.
2	Clster-nodo1.	Nodo 1 OpenLdap Samba.
3	Clster-nodo2.	Nodo 2 OpenLdap Samba.
4	Clster-nodo3.	Nodo 3 OpenLdap Samba.
5	Openfiler.	Administración de almacenamiento compartido.

Tabla 2.1 - Equipos Virtuales para el entorno de Alta Disponibilidad OpenLdap – Samba

Configuración del entorno de red para los equipos *en el* entorno de Alta Disponibilidad OpenLdap – Samba.

No	Nombre	Hostname	Dirección IP	Mascara de Red	Puerta de enlace
1	Clster-manager.	clsterm.jorgearmijo.com	192.168.12.10	255.255.0.0	192.168.6.1
2	Clster-nodo1.	clster1.jorgearmijo.com	192.168.12.1	255.255.0.0	192.168.6.1
3	Clster-nodo2.	clster2.jorgearmijo.com	192.168.12.2	255.255.0.0	192.168.6.1

No	Nombre	Hostname	Dirección IP	Mascara de Red	Puerta de enlace
4	Clster-nodo3.	clster3.jorgearmijo.com	192.168.12.3	255.255.0.0	192.168.6.1
5	Openfiler.	openfiler.jorgearmijo.com	192.168.12.30	255.255.0.0	192.168.6.1

Tabla 2.2 Configuración del entorno de red para los equipos en el entorno de Alta Disponibilidad OpenLdap – Samba

2.1.1 Instalación del Sistema Operativo.

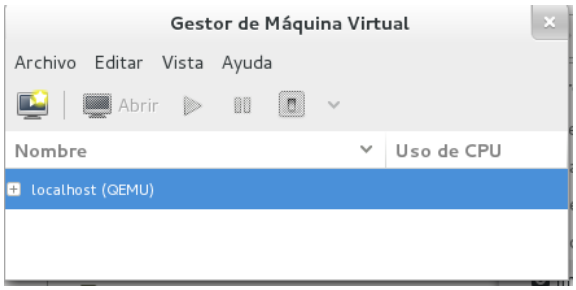
Para la instalación del sistema operativo RHEL 6.5 se debe tener consideraciones sobre el espacio de disco, el tipo de servidor que se va a configurar y principalmente el esquema de particionamiento que se utilizara para cada uno de los nodos.

Ingresar a la plataforma de Virtualización KV.M.

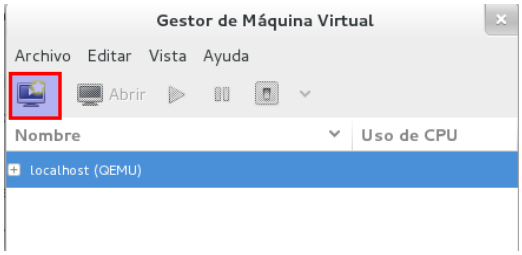
A través de línea de comandos ejecutamos:

```
# virt-manager
```

Se desplegará la interfaz de administración del K.V.M.

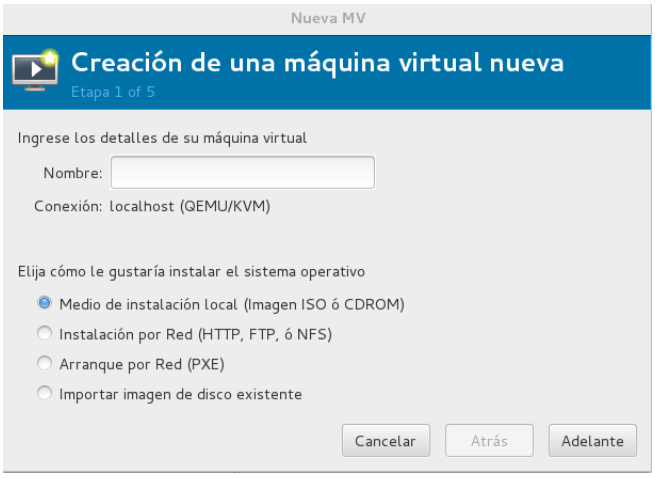


Se seleccionará del menú principal el icono para la creación de máquinas virtuales.



Se abrirá una venta nueva para la creación de la máquina virtual sobre la cual se definirá el nombre de la maquina a ser creada.

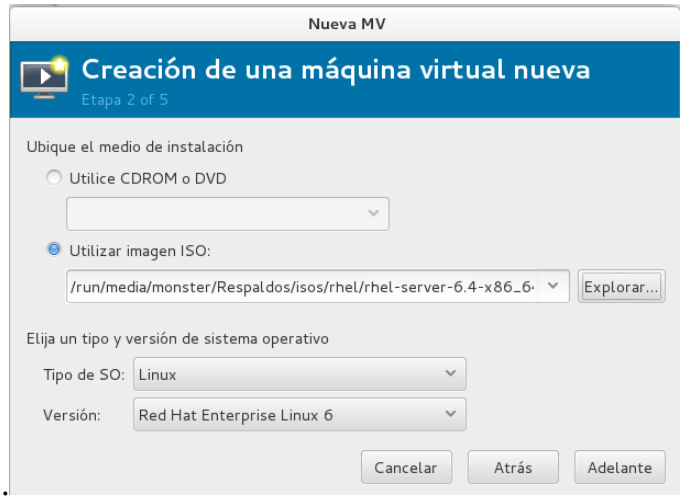
Nota: Se debe utilizar nombres que describan el funcionamiento del servidor.



Ingresar el nombre para identificar el respectivo Servidor RHEL6.5_x86_64 Virtualizado según la tabla 2.2 definida previamente.

2.1.1.1 Selección del medio de Instalación y versión del Sistema Operativo.

Selección del medio de instalación en este caso se utilizará una imagen ISO del Sistema Operativo RHEL6.5_x86_64.



En este caso en se ha asignado una Imagen ISO como medio de Instalación y el Tipo de Sistema Operativo “Linux” en versión “Red Hat Enterprise Linux 6”. Se puede optar por usar la unidad de DVD como alternativa en caso no disponer de la Imagen ISO.

2.1.1.2 Asignación de memoria.

Para la asignación de memoria dependerá de las características físicas de los equipos sobre cual se desarrolle la implementación de esta guía.

Para este caso en particular se asignará 1024Gb de memoria Ram.

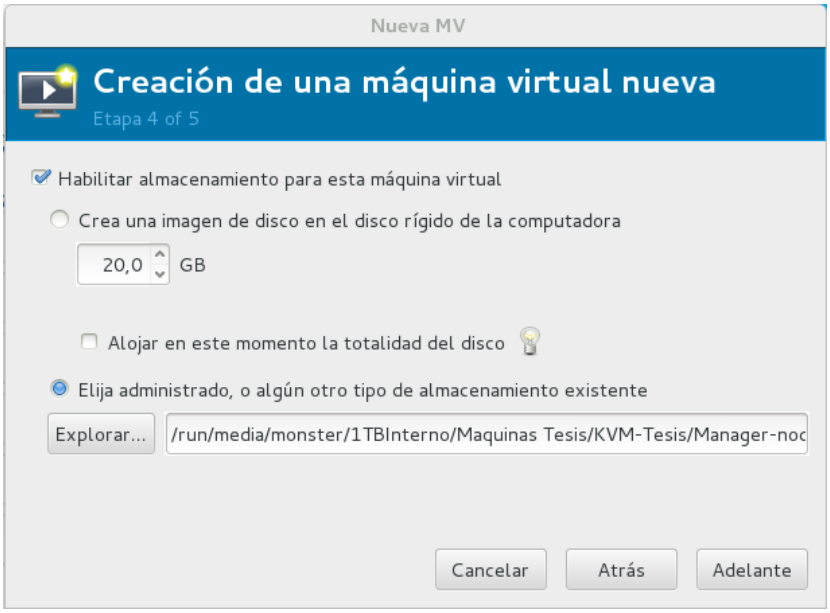
Nota: La configuración de memoria dependerá de la memoria Ram física del equipo sobre el cual estamos realizando la configuración del entorno de Alta disponibilidad.

2.1.1.3 Asignación del espacio de almacenamiento.

Para este caso en particular se asignara 20Gb para el disco duro del sistema virtualizado. Se procederá a reservar la cantidad de disco duro que será asignado y la ruta sobre la cual se almacenara.

El tipo de almacenamiento para el disco duro puede ser de dos tipos:

- Reservado Dinámicamente.
- Tamaño fijo.



En este caso se escogerá la opción "Tamaño fijo" para hacer la reserva del total del espacio de disco en la creación de la máquina virtual.

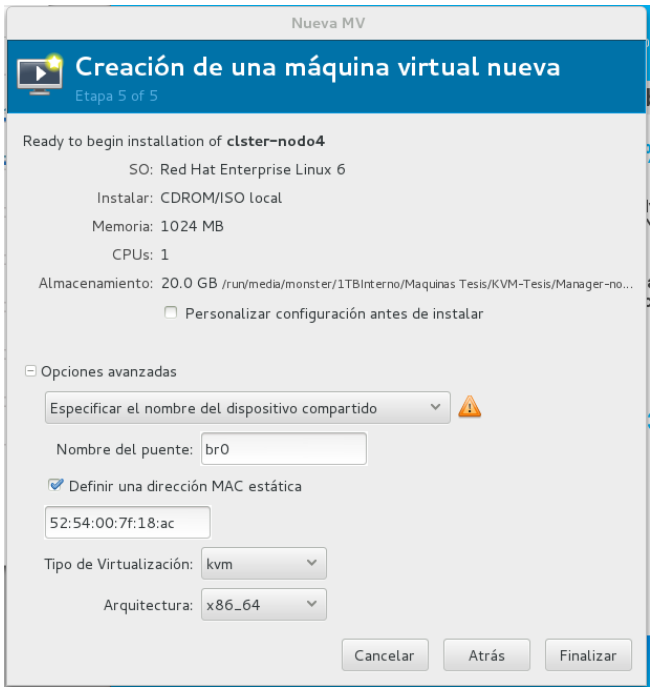
Para la asignación del espacio de almacenamiento dependerá de las características físicas de los equipos sobre cual se desarrolle la implementación de esta guía.

2.1.1.4 Configuración de interface de red.

Se procederá a seleccionar la interfaz de red sobre la cual tendremos acceso a los recursos compartidos.

En este caso se procederá por la opción llamada "Especificar el nombre del dispositivo compartido" en la cual se describirá el medio por el cual se tendrá acceso a la red interna.

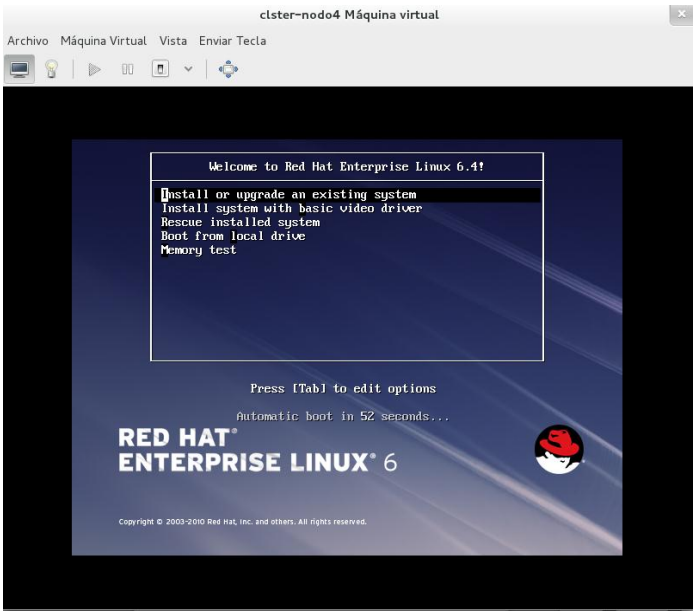
Para el caso se seleccionara en el “Nombre del puente” “br0”.



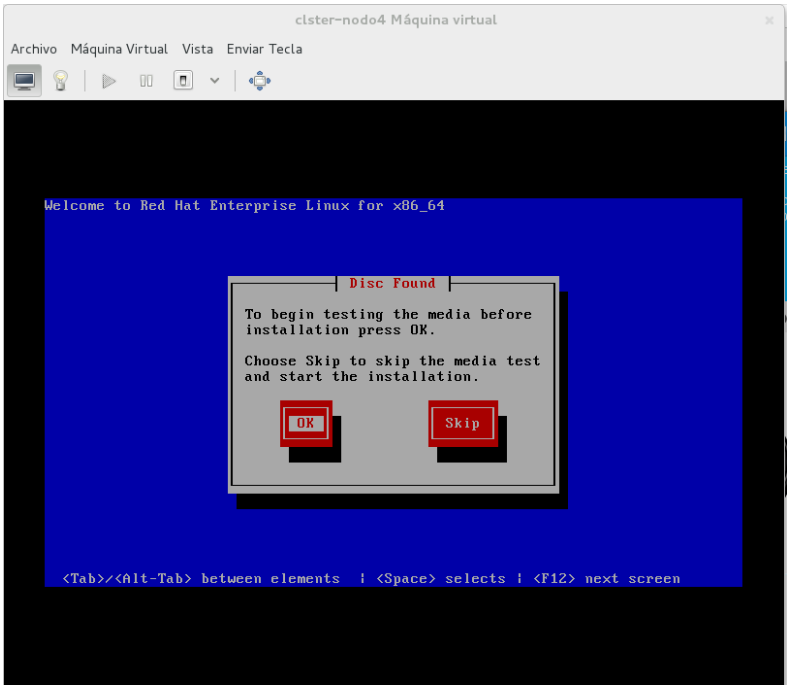
2.1.1.5 Instalación del Sistema Operativo.

Una vez realizadas la configuración de Disco y de Interfaz de red procederemos con la instalación del sistema virtualizado en la cual se desplegará el menú de instalación del sistema Red Hat Enterprise Linux versión 6.5.

Seleccionaremos la primera opción **“Install or upgrade an existing system”**



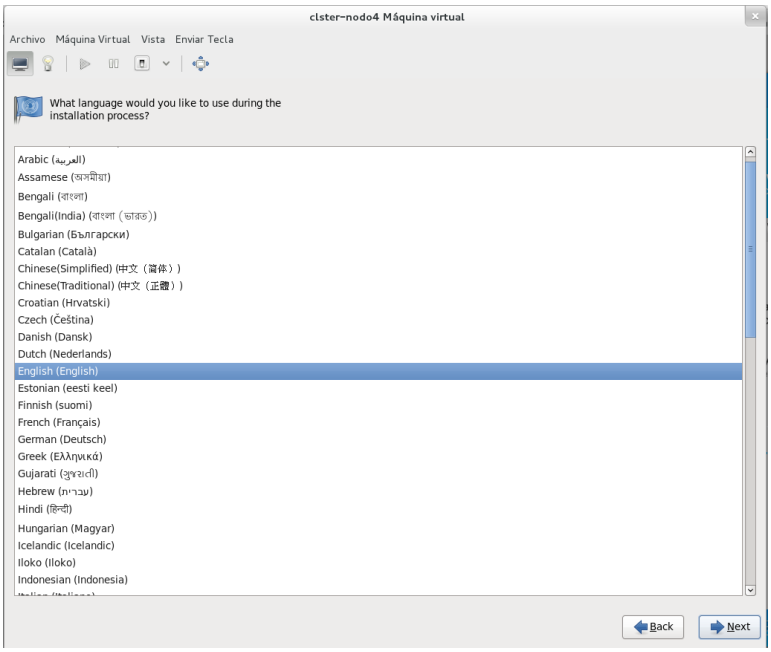
Como se está usando una imagen ISO de RHEL6.5_x86_64 no se realizará la comprobación del medio de instalación.



Con este procedimiento se accederá al asistente de instalación llamado anaconda para realizar la configuración del sistema.

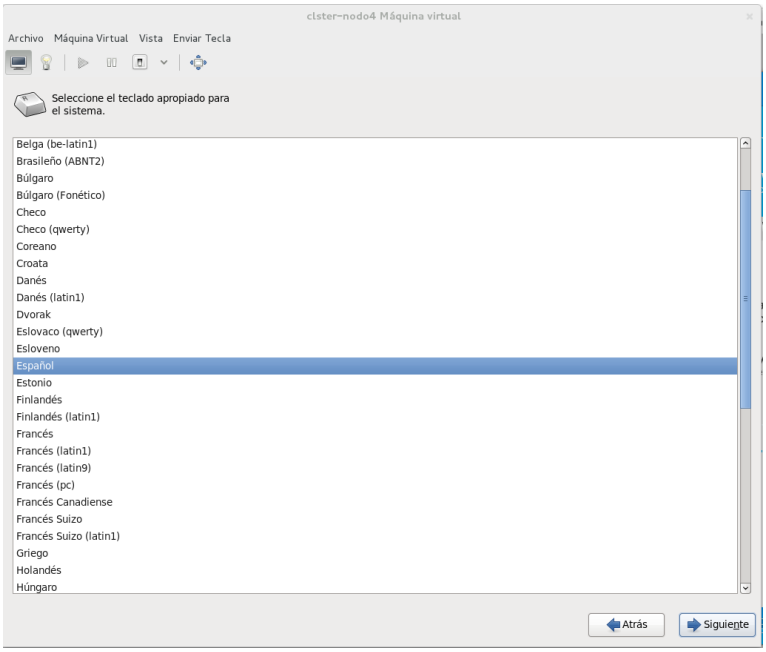
2.1.1.6 Seleccionar Idioma para la instalación del Sistema Operativo.

Se seleccionará como idioma por defeco para la instalación del Sistema Operativo “Español”



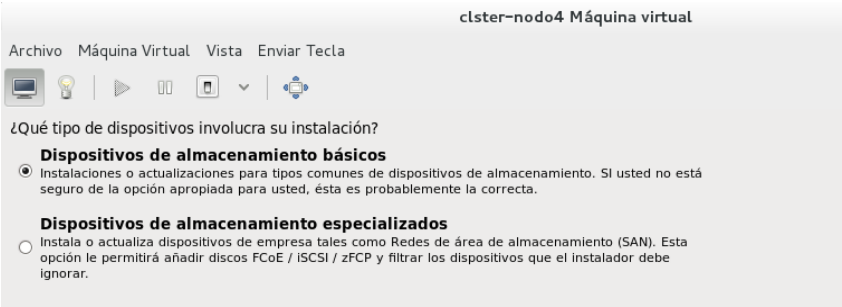
2.1.1.7 Seleccionar el teclado apropiado.

Se seleccionará como idioma por defeco para el teclado “Español”.



2.1.1.8 Seleccionar el o los dispositivos de disco para realizar la instalación.

Seleccionar la opción que corresponda al medio donde se realizará la instalación en este caso seleccionaremos “Dispositivos de almacenamiento básicos”

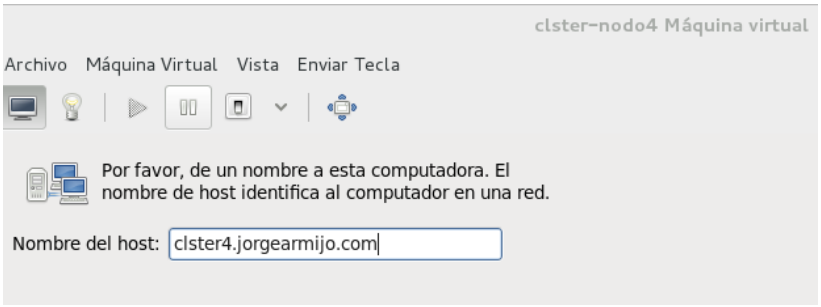


Presentará una ventana de notificación indicando que el dispositivo de disco duro seleccionado será formateado y preparado para realizar una instalación desde cero en el disco asignado.

Nota: Descartaremos los datos para proceder con un tipo de instalación nueva sobre los equipos. En caso de haber un sistema operativo previamente cargado esta opción la eliminará.

2.1.1.9 Configuración de hostname para el sistema virtualizado.

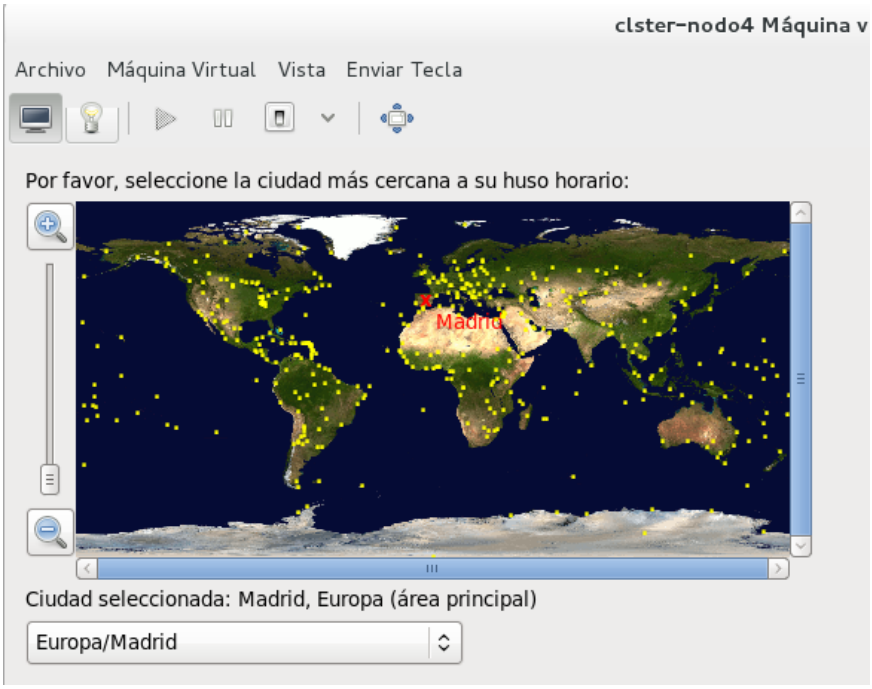
El hostname será la el nombre con el cual el servidor podrá ser identificado en el segmento de red configurado.



Nota: La configuración de red se realizará posterior a la instalación del sistema operativo para cumplir con los requerimientos del entorno de alta disponibilidad.

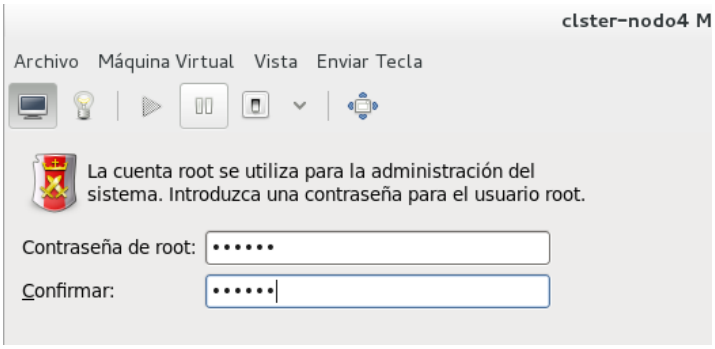
2.1.1.10 Configuración de la zona horaria.

Por medio del mapa seleccionaremos la ubicación más cercana "America/Guayaquil".



2.1.1.11 Ingreso de la contraseña de root

Definición de la contraseña para el súper usuario del sistema operativo.



2.1.1.12 Particionamiento del Sistema Operativo.

Se seleccionará un tipo de particionamiento específico para cada uno de los servidores.

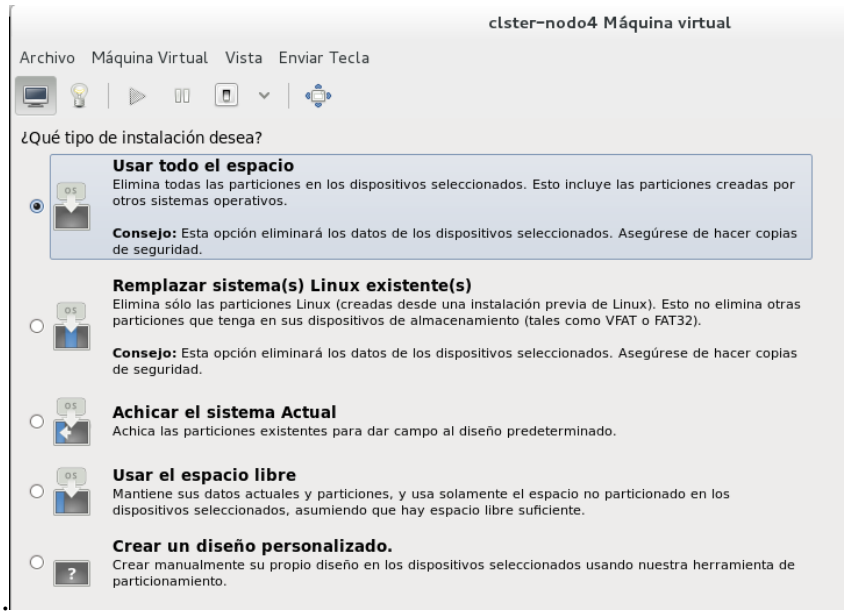
En este caso en particular para el servidor OpenLdap-Samba la distribución será:

Particionamiento del Sistema Operativo OpenLdap-Samba		
Punto de montaje	**Nombre**	**Tamaño en GB**
/boot	boot	500Mb
/root	root	10GB
/var/lib/ldap	ldap	5GB
/home	home	5GB

Tabla 2.3 Particionamiento del Sistema Operativo OpenLdap-Samba

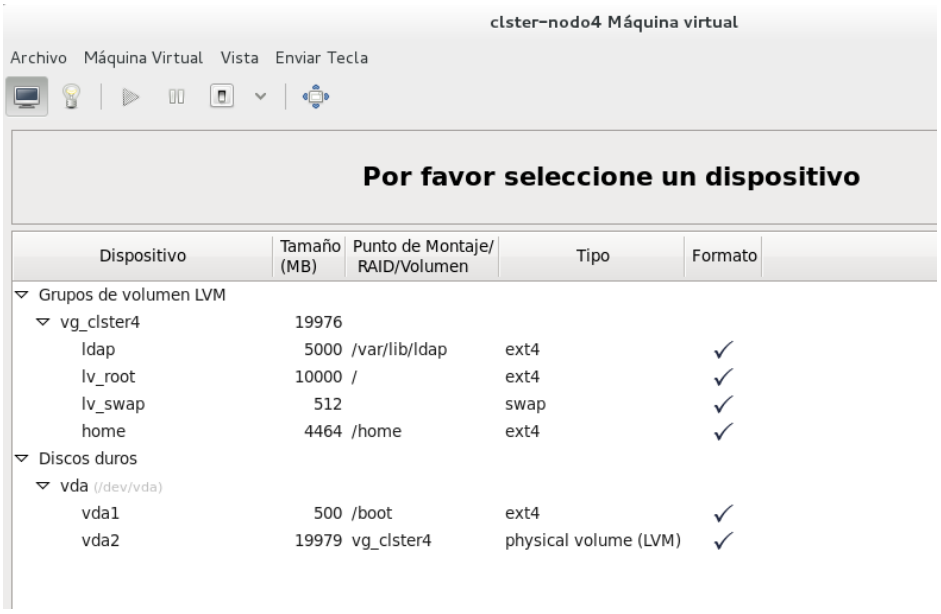
Para realizar la instalación de un sistema operativo nuevo escogemos la primera opción de **"Usar todo el espacio"** y activamos la casilla de **"Revisar y modificar el diseño de particiones"** como se muestra a continuación.

Con esta opcion nos permitira definir el esquema de particionamiento del Servidor.



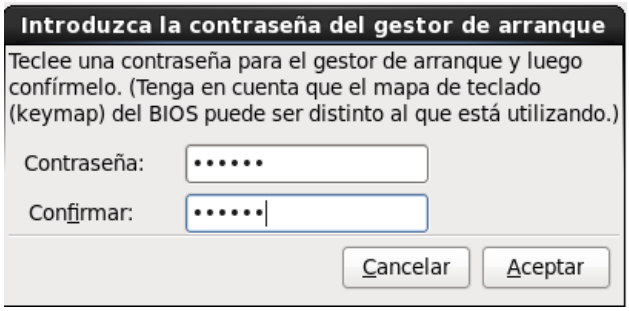
Seleccionamos la casilla de “Revisar y modificar el diseño de particiones para realizar la configuración para los servidores OpenLdap – Samba”

Ingresamos los valores respectivos para el particionamiento del Sistema Operativo descritos en la tabla 2.3



2.1.1.13 Configuración de contraseña para el grub.

Por temas de seguridad es mejor definir una contraseña para evitar vulnerabilidades en el servidor, para eso marcaremos la opción **"Usar la contraseña del gestor de arranque".**

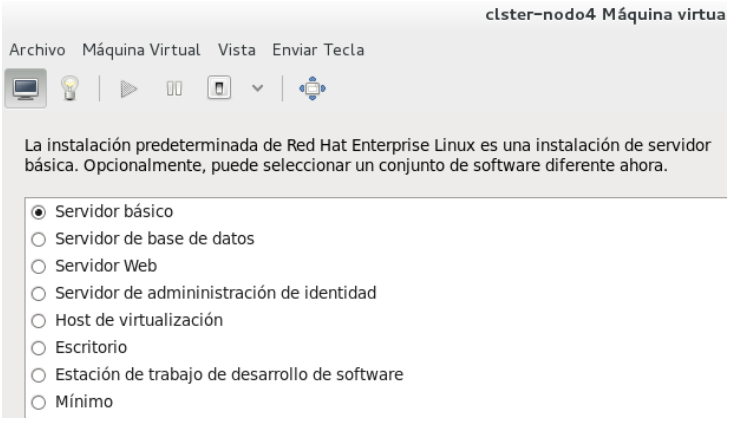


Ingresamos la contraseña a ser definida "redhat"

Nota: Una vez en producción las contraseñas deben de ser cambiadas.

2.1.1.14 Seleccionar el tipo de servidor que se instalara

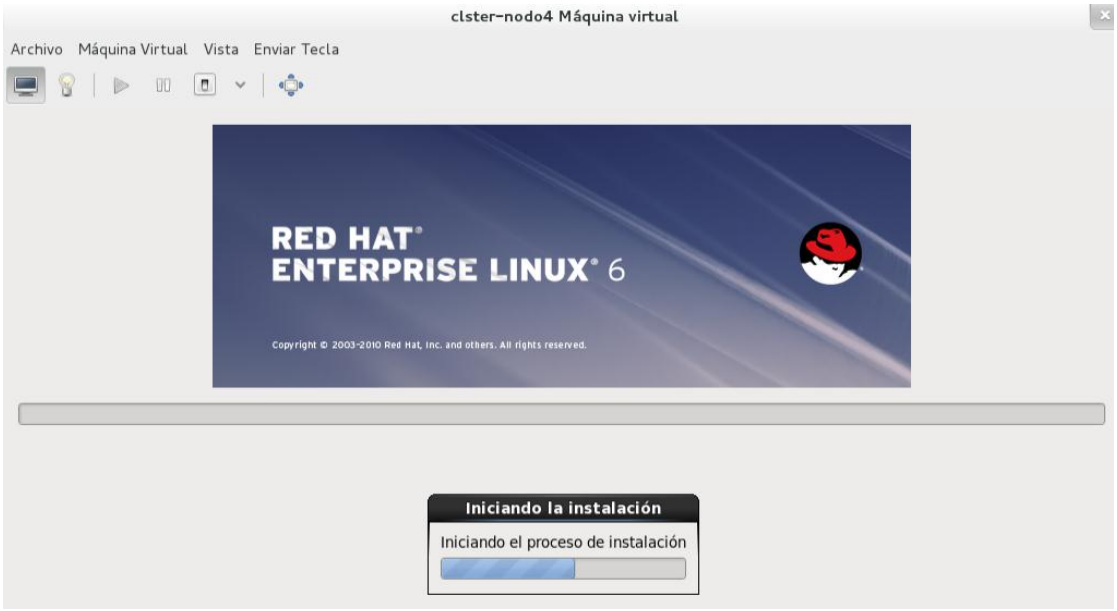
En el menú de opciones:



Una vez definida la contraseña del super usuario se procederá por seleccionar el tipo de servidor a instalar en este caso se escogera la opción Servidor Básico.

Se aceptara las configuraciones definidas para este tipo de servidor y procederemos con la comprobación de dependencias de los paquetes a ser instalados.

El proceso de instalación tomará alrededor de 20 minutos para finalizar.



Al final del proceso de instalación se tendrá un mensaje de culminación de la instalación y un mensaje de reinicio.

2.1.2 Configuración del Sistema Operativo.

2.1.2.1 Configuración de la interface de red

Edición del archivo /etc/sysconfig/network-scripts/ifcfg-eth0

```
# vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

Habilitamos: ONBOOT =yes

Deshabilitamos NM_MANAGER=no

Agregamos las siguientes líneas ejemplo para el nodo 4:

BOOTPROTO=static

IPADDR=192.168.12.4

NETMASK=255.255.0.0

GATEWAY=192.168.6.1

DNS1=192.168.6.1

Nota: Las configuraciones de red para cada nodo serán realizadas de acuerdo con la Tabla 2.2

Reiniciamos la configuración de red ejecutando en un terminal

```
# service network restart
```

2.1.2.2 Modificación para la resolución de nombres.

Edición del archivo /etc/hosts

```
# vim /etc/hosts
```

En este archivo agregaremos para cada uno de los nodos que intervendrían en el entorno de alta disponibilidad.

```
192.168.12.10 clsterm.jorgearmijo.com clsterm
192.168.12.1 clster1.jorgearmijo.com clster1
192.168.12.2 clster2.jorgearmijo.com clster2
192.168.12.3 clster3.jorgearmijo.com clster3
192.168.12.4 clster4.jorgearmijo.com clster4
192.168.12.30 openfiler.jorgearmijo.com openfiler
```

Nota: En este archivo declararemos los nombres de los servidores y sus direcciones IP.

2.1.2.3 Configuración del repositorio de datos.

Para la configuración del repositorio de datos crearemos el archivo /etc/yum.repos.d/local.repo El archivo contendrá el siguiente texto que habilitara los repositorios de paquetes necesarios para la instalación del entorno de alta disponibilidad de los servicios del OpenLdap y Samba.

```
# touch  /etc/yum.repos.d/local.repo
```

```
[base]
name=Local
baseurl=file:///media/rhel/Server
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[HighAvailability]
name=HighAvailability
baseurl=file:///media/rhel/HighAvailability
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[LoadBalancer]
name=LoadBalancer
baseurl=file:///media/rhel/LoadBalancer
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[ResilientStorage]
name=ResilientStorage
baseurl=file:///media/rhel/ResilientStorage
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[ScalableFileSystem]
name=ResilientStorage
baseurl=file:///media/rhel/ScalableFileSystem
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

Para habilitar los repositorios se ejecutará en un termina el comando yum repolist.

```
# yum repolist
```

Se debe presentar una salida similar a la siguiente:

```
[root@clster1]# yum repolist

Loaded plugins: product-id, security, subscription-manager
repo id                    repo name                  status
EPEL                       EPEL                       8
HighAvailability           HighAvailability           56
LoadBalancer               LoadBalancer               4
ResilientStorage           ResilientStorage           62
ScalableFileSystem         ResilientStorage           7
base                       Local                      3.648
repolist: 3.785
```

2.1.2.4 Configuración de almacenamiento compartido para OpenLdap.

Para la configuración de almacenamiento compartido referirse al *Anexo "1"* donde se muestra la instalación y configuración de un servidor Openfiler quien proveerá el sistema de almacenamiento compartido para el clúster de OpenLdap.

En los nodos definidos para el entorno de alta disponibilidad en un terminal ejecutar:

```
# yum install -y gfs2-utils iscsi-initiator-utils
```

Para iniciar los servicios de iscsi del servidor:

```
# /etc/init.d/iscsi start ; /etc/init.d/iscsid start
```

Para que estén disponibles a un reinicio del servidor:

```
# chkconfig iscsi on ; chkconfig iscsid on
```

Para la identificación de discos nuevos ejecutamos en cada nodo.

```
# iscsiadm --mode discovery --type sendtargets --portal 192.168.12.30
```

En los nodos definidos se debe reiniciar los servicios de iscsi para identificar el ISCSI.

```
# /etc/init.d/iscsi restart
```

Para identificar la partición presentada con iscsi se debe ejecutar en un terminal:

```
# cat /proc/partitions
```

Con la ejecución de este comando podemos identificar los almacenamientos compartidos por el servidor de ISCSI.

```
252        0    20971520 vda
 252       1    512000     vda1
 252       2    20458496 vda2
   8       0    5144576   sda
   8       16   7176192   sdb
```

Del resultado anterior podemos identificar que están presentados dos volúmenes descritos con el nombre de sda y sdb para la data de los servicios de OpenLdap y de Samba respectivamente.

Nota: El valor de la tercera columna nos permite identificar el tamaño del volumen presentado.

Para la creación de un disco físico para OpenLdap se ejecutará en la terminal:

```
# pvcreate /dev/sda
  Physical volume "/dev/sda" successfully created
```

Para la creación de un Grupo de Volúmenes Lógicos para OpenLdap se ejecutará en la terminal:

```
# vgcreate openldap /dev/sda
  Volume group "openldap" successfully created
```

Para la creación del Volumen Lógico para almacenar la información del OpenLdap se ejecutará en la terminal:

```
# lvcreate -n varlibldap -l +100%FREE openldap
  Logical volume "varlibldap" created
```

Para la creación del punto de montaje se ejecutará en la terminal:

```
# mkdir /var/lib/ldap
```

Para definir el punto de montaje automático al inicio del servidor se deberá agregar en el archivo /etc/fstab las siguientes líneas:

```
/dev/openldap/varlibldap /var/lib/ldap gfs2 defaults,noatime,nodiratime,quota=off 0 0
```

NOTA: Para dar formato a la partición del ldap debe estar creado el clúster y definido el número de nodos que intervendrán en el mismo. Procederemos a la parte de la instalación y creación del clúster en la guía en el numeral 2.7.

Una vez definido el clúster y sus nodos en el terminal ejecutar en un terminal:

```
# mkfs.gfs2 -p lock_dlm -t OpenLdap-Samba:gfs-openldap -j 16 /dev/openldap/varlibldap
```

Dónde:

OpenLdap-Samba: Corresponde al nombre del clúster.

Gfs-opendldap: Corresponde al nombre del sistema de archivos del clúster.

-j 16: Corresponde a la cantidad máxima de nodos que pueden ser establecidos en un clúster de Red Hat.

Con la ejecución del comando anterior de procederá a dar formato en el punto de montaje con el sistema de archivos compartido gfs: /dev/openldap/varlibldap /var/lib/ldap
En la terminal se tendrá una salida similar a la siguiente:

```
This will destroy any data on /dev/openldap/varlibldap.
It appears to contain: symbolic link to `../dm-3'

Are you sure you want to proceed? [y/n] y

Device:                 /dev/openldap/varlibldap
Blocksize:              4096
Device Size             4,90 GB (1285120 blocks)
Filesystem Size:        4,90 GB (1285117 blocks)
Journals:               16
Resource Groups:        20
Locking Protocol:       "lock_dlm"
Lock Table:             "OpenLdap-Samba:gfs-openldap"
UUID:                   fe8f1513-7291-9c06-f979-7661ed6e1a91
```

2.1.2.5 Configuración de almacenamiento compartido para Samba.

Para la configuración de almacenamiento compartido referirse al Anexo "1" donde se muestra la instalación y configuración de un servidor Openfiler quien proveerá el sistema de almacenamiento compartido para el clúster de Samba.

Una vez identificados los discos nuevos para el almacenamiento compartido y agregado el disco sda para el OpenLdap resta agregar el segundo disco sdb para el almacenamiento de la data de samba.

Para la identificación de discos nuevos ejecutamos en cada nodo.

```
# iscsiadm --mode discovery --type sendtargets --portal 192.168.12.30
```

Reiniciamos los servicios de iscsi

```
# /etc/init.d/iscsi restart
```

Para identificar la partición presentada con iscsi se debe ejecutar en un terminal:

```
# cat /proc/partitions
```

Con la ejecución de este comando podemos identificar los almacenamientos compartidos por el servidor de ISCSI.

```
252        0    20971520 vda
 252       1    512000     vda1
 252       2    20458496 vda2
   8       0    5144576   sda
   8       16   7176192   sdb
```

Del resultado anterior podemos identificar que están presentados dos volúmenes descritos con el nombre de sda y sdb para la data de los servicios de OpenLdap y de Samba respectivamente.

Nota: El valor de la tercera columna nos permite identificar el tamaño del volumen presentado respectivamente.

Para la creación de un Grupo de Volúmenes Lógicos para Samba ejecutamos en un terminal:

```
# vgcreate samba /dev/sda
  Volume group "samba" successfully created
```

Para la creación del Volumen Lógico para almacenar la información del Samba ejecutamos en un terminal:

```
# lvcreate -n samba-data -l +100%FREE samba
  Logical volume "samba-data" created
```

Creación del punto de montaje para almacenar la información a compartir mediante Samba ejecutar en un terminal:

```
# mkdir /samba-archivos/
```

Definición del punto de montaje automático al inicio del servidor agregando en el archivo /etc/fstab las siguientes líneas:

```
/dev/samba/samba-data /samba-archivos gfs2 defaults,noatime,nodiratime,quota=off 0 0
```

Una vez definido el clúster y sus nodos en el terminal ejecutar en un terminal:

```
# mkfs.gfs2 -p lock_dlm -t OpenLdap-Samba:gfs-samba -j 16 /dev/samba/samba-data
```

Dónde:

- **OpenLdap-Samba:** Corresponde al nombre del clúster.
- **Gfs-opendldap:** Corresponde al nombre del sistema de archivos del clúster.
- **-j 16:** Corresponde a la cantidad máxima de nodos que pueden ser establecidos en un clúster de Red Hat.
- **Punto de montaje del sistema gfs**: /dev/samba/samba-data /samba-archivos

Con la ejecución del comando anterior de procederá a dar formato en el punto de montaje con el sistema de archivos compartido gfs: /dev/openldap/varlibldap /var/lib/ldap
En la terminal se tendrá una salida similar a la siguiente:

```
This will destroy any data on /dev/samba/samba-data.
It appears to contain: symbolic link to `../dm-2'

Are you sure you want to proceed? [y/n] y

Device:                  /dev/samba/samba-data
Blocksize:               4096
Device Size              6,84 GB (1793024 blocks)
Filesystem Size:         6,84 GB (1793021 blocks)
Journals:                16
Resource Groups:         28
Locking Protocol:        "lock_dlm"
Lock Table:              "OpenLdap-Samba:gfs-samba"
UUID:                    50cbc114-be5d-8c76-fd46-d821ae56d045
```

Nota: Una vez presentado los volúmenes de almacenamiento compartido seguiremos con el punto 2.2 de la guía.

2.2 Instalación Protocolo Ligero de Acceso a Directorios LDAP.

2.2.1 Instalación del OpenLdap.

Para la instalación del OpenLdap procederemos con los siguientes pasos:

```
# yum -y install openldap openldap-clients openldap-servers nss-pam-ldapd authconfig
authconfig-gtk migrationtools
```

2.2.2 Configuración OpenLdap.

Se debe editar el archivo /etc/sysconfig/ldap y verificar que estén sin comentar las siguientes líneas.

```
SLAPD_LDAP=yes
SLAPD_LDAPI=yes
SLAPD_LDAPS=yes
```

Editar el archivo /etc/openldap/ldap.conf y proceder a realizar las configuraciones principales para el acceso de nuestro Directorio Activo OpenLdap. En este caso el directorio Activo será identificado por dc=jorge,dc=armijo,dc=com. Estos valores pueden ser modificados de acuerdo a las necesidades de implementación de la Organización.

En este caso:

```
TLS_CACERTDIR /etc/openldap/cacerts
URI ldap://192.168.12.20/ #IP del cluster
BASE dc=jorge,dc=armijo,dc=com
TLS_REQCERT NEVER
```

Se debe copiar el archivo de configuración de parámetros predefinidos para el tamaño máximo de los logs de transacciones que generará el OpenLdap del directorio /usr/share/openldap-servers/DB_CONFIG.example a el directorio del OpenLdap.

En un terminal ejecutar:

```
# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

Se debe validar que las siguientes opciones estén sin comentar en el archivo /var/lib/ldap/DB_CONFIG.

```
set_cachesize 0 268435456 1
set_lg_regionmax 262144
set_lg_bsize 2097152
```

Se debe cambiar los permisos de propiedad de usuario y grupo del directorio /var/lib/ldap/ para el usuario ldap que se creó automáticamente en la instalación de paquetes del OpenLdap.

```
# chown -R ldap:ldap /var/lib/ldap/*
```

Editar el archivo de configuración del OpenLdap.

```
#  vim /etc/openldap/slapd.conf
```

El archivo de configuración de OpenLdap debe tener la siguiente estructura.

Habilitamos los esquemas de información predefinidos por la Instalación del OpenLdap.

```
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema
include         /etc/openldap/schema/samba.schema
```

Se debe habilitar las credenciales de autenticidad para conexiones seguras TLS/SSL.

```
TLSCertificateFile /etc/pki/tls/certs/slapd.pem
TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem
```

Para habilitar los permisos de escritura sobre la información del directorio se debe realizar la siguiente configuración.

```
access to *
 by
group/groupOfNames/member="cn=SuperAdmins,ou=Group,dc=jorge,dc=armijo,dc=com
" write  by * break

access to *
        by self write
        by users read
        by anonymous read
        by * none
```

Parámetros para la definición del Directorio Activo

```
database        bdb
suffix          "dc=jorge,dc=armijo,dc=com"
checkpoint      1024 15
rootdn          "cn=Manager,dc=jorge,dc=armijo,dc=com"
```

Configuración de la clave de administración del OpenLdap. “rootpw” para realizarla se debe ejecutar en un terminal:

```
#  slappasswd -s JorgeArmijo0812x
```

La ejecución de este comando nos devolverá:

```
rootpw          {SSHA}4xcnXnSdiiBSVWQEwzwrs02FmqdK4W1F
```

Este valor se debe reemplazar en el archivo /etc/openldap/slapd.conf por el valor definido por defecto como “secret” por el valor “{SSHA}4xcnXnSdiiBSVWQEwzwrs02FmqdK4W1F” obtenido en la terminal.

Se debe habilitar los parámetros de búsqueda para los objetos definidos en los esquemas incluidos.

```
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
index entryCSN                          eq
index entryUUID                         eq
index default                           sub
```

Definir el número máximo de entidades que devolverá la búsqueda de información sobre el directorio activo.

```
sizelimit 80000
```

Una vez definidos los parámetros previos procedemos a guardar los cambios realizados en el archivo de configuración de OpenLdap. A continuación se debe cambiar los permisos de propiedad de usuario y grupo del directorio /etc/openldap/slapd.d para el usuario ldap que se creó automáticamente en la instalación de paquetes del OpenLdap.

```
# chown -R ldap:ldap /etc/openldap/slapd.d
```

Previamente el contenido del directorio /etc/openldap/slapd.d/ para la creación de los archivos de definición del directorio activo que están descritas en el archivo /etc/openldap/slapd.conf. se debe tener vacio para lo cual ejecutamos en un terminal lo siguiente:

```
# rm -rf /etc/openldap/slapd.d/*
```

Para definir la estructura básica del directorio activo se debe crear un archivo inicial el mismo estará almacenado en el directorio /home temporalmente.

```
# vim /home/configuracion_inicial.ldif
```

El contenido del archivo inicial de configuración será por el cual procederemos a definir los parámetros básicos de información para el Directorio Activo el cual contendrá lo siguiente.

```
dn: dc=jorge,dc=armijo,dc=com
objectclass: dcObject
objectclass: organization
o: Tesis Jorge Armijo 2013
dc: ORGANIZACION
```

Para la creación de la estructura básica del directorio activo se debe ejecutar en un terminal:

```
# slapadd -l /home/configuracion_inicial.ldif
```

Para la validación de la configuración del archivo de configuración del Directorio Activo se debe ejecutar en un terminal:

```
# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
```

Debemos tener una salida de pantalla similar a la siguiente ***"config file testing succeeded"*** este mensaje nos indicara que la configuración del archivo /etc/openldap/slapd.conf es la correcta para la información inicial necesaria para llenar de información al Directorio Activo.
Una vez realizados los pasos de configuración previos se debe proceder a iniciar el servicio del ldap para ingresar información del directorio activo para lo cual en un terminal ejecutar:

```
# service slapd start
```

Para agregar la primera información del Directorio Activo se debe crear un archivo con las configuraciones iniciales de usuarios y grupos que estará almacenado en el archivo /etc/openldap/base.ldif, para hacerlo efectivo se debe ejecutar en el terminal:

```
ldapadd -x -W -c -D "cn=Manager,dc=jorge,dc=armijo,dc=com" -f /etc/openldap/base.ldif
```

Una realizada la configuración básica se observará una salida en el terminal similar a la siguiente:

```
[root@clster1 ]# ldapadd -x -W -c -D "cn=Manager,dc=jorge,dc=armijo,dc=com" -f
/etc/openldap/base.ldif
Enter LDAP Password:
adding new entry "dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Hosts,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Rpc,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Services,dc=jorge,dc=armijo,dc=com"
adding new entry "nisMapName=netgroup.byuser,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Mounts,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Networks,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=People,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Group,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Netgroup,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Protocols,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Aliases,dc=jorge,dc=armijo,dc=com"
adding new entry "nisMapName=netgroup.byhost,dc=jorge,dc=armijo,dc=com"
```

Una vez realizado estos procedimientos podemos proceder con la instalación y configuración del Controlador de Dominio Primario.

2.3 Instalación de un Controlador de Dominio Primario

2.3.1 Instalación Controlador de Dominio Primario.

Para la instalación del Software para el controlador de dominio se debe ejecutar en un terminal:

```
# yum install samba samba-winbind-clients samba-common  samba-winbind samba-client
```

Con este comando se instalaran los paquetes necesarios para realizar la configuración del Servicio de Samba para realizar la compartición de archivos entre los equipos Windows simulando un dominio Windows NT.

2.3.2 Configuraciones Controlador de Dominio Primario.

Para la configuración del controlador de Dominio Primario se debe editar el archivo de configuración de samba /etc/samba/smb.conf de la siguiente forma:

Ejecutar en un terminal para acceder a la edición del archivo.

```
# vim /etc/samba/smb.conf
```

Dentro de este archivo encontraremos tres secciones principales de configuración:

- Global.
- Netlogon.
- Profiles.

Dentro de cada una de estas tres secciones se realiza la configuración para definir un servidor samba como PDC integrado con OpenLdap para la autenticidad de usuarios en el dominio llamado ORGANIZACION

2.3.2.1 Global.

Configuraciones Globales para el Controlador de Dominio Principal.

Definición del Dominio para interactuar con el OpenLdap.

```
[global]
        workgroup = ORGANIZACION
        netbios name = ORGANIZACION
        server string = Samba Server %v
```

Definición de parámetros para la autentificación de usuarios.

```
        security = user
        encrypt passwords = Yes
        obey pam restrictions = yes
        unix password sync = yes
```

Definición de parámetros para la conexión con OpenLdap.

```
        ldap admin dn = cn=Manager,dc=jorge,dc=armijo,dc=com
        ldap suffix = dc=jorge,dc=armijo,dc=com
        ldap group suffix = ou=Group
        ldap user suffix = ou=People
        ldap machine suffix = ou=Computers
        ldap ssl = no
```

Definición de parámetros para la compartición de impresoras de red.

```
load printers = Yes
printing = cups
printcap name = cups
deadtime = 10
```

Definición de parámetros para el controlador de dominio

```
logon script = logon.bat
logon drive = H:
logon home = \\%L\%u\.profile
logon path = \\%L\profiles\%u
domain logons = Yes
domain master = Yes
os level = 120
preferred master = Yes
wins support = yes
passdb backend = ldapsam:ldap://127.0.0.1/
create mask = 0640
directory mask = 0750
nt acl support = Yes
```

Definición de parámetros para la creación de usuarios y de máquinas en el Dominio a través de la herramienta smblap-tools.

```
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
```

2.3.2.2 Netlogon.

Configuraciones para el netlogon que almacenara los scripts de autentificación de los clientes Windows Xp, 7, 8.

```
path = /samba-archivos/home/netlogon/
browseable = No
read only = yes
```

2.3.2.3 Profiles.

Configuraciones necesarias para el almacenamiento de los perfiles de usuario de los clientes Windows Xp, 7, 8.

```
path = /samba-archivos/home/profiles
read only = no
create mask = 0600
directory mask = 0700
```

2.4 Archivos de configuración de Samba y LDAP.

2.4.1 Instalación y Configuración de las herramientas smbldap-tools

La instalación del paquete smbldap-tools permitirá realizar la integración de OpenLdap y Samba a través de sus herramientas para la administración en conjunto del Dominio en Samba y del Directorio Activo con Openldap, permitiéndonos emular un entorno de domino Windows NT para el acceso de estaciones de trabajo Windows Xp, Windows 7, Windows 8 Windows Server 2003, Windows Server 2008 y Linux.

```
path = /samba-archivos/home/profiles
read only = no
create mask = 0600
directory mask = 0700
```

2.4.2 Configuración del smbldap.conf

El archivo de configuración del smbladp-tools se encuentra en /etc/smbldap-tools/smbldap.conf y debe tener los siguientes campos en los cuales se describen las credenciales de autenticidad para el OpenLdap y el Samba.

Definición Global de parámetros para Dominio

```
SID="S-1-5-21-2323392562-1448967901-2038806033"
sambaDomain="ORGANIZACION"
slaveLDAP="127.0.0.1"
masterLDAP="192.168.12.20"  # ip del cluster
```

Definición para la conexión con OpenLdap

```
masterPort="389"
slavePort="389"
ldapTLS="0"
verify=""
cafile=""
clientcert=""
clientkey=""
suffix="dc=jorge,dc=armijo,dc=com"
```

Definición de parámetros de administración del OpenLdap.

```
usersdn="ou=People,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Group,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=ORGANIZACION,${suffix}"
scope="sub"
hash_encrypt="SSHA"
crypt_salt_format=""
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"
userSmbHome="\\ORGANIZACION\%U"
userProfile="\\ORGANIZACION\profiles\%U"
userHomeDrive="H:"
userScript="logon.bat"
mailDomain=""
```

2.4.3 Configuración del smbldap_bind.conf

Configuración de las credenciales de autenticidad para el servidor Principal y el servidor secundario.

```
slaveDN="cn=Manager,dc=jorge,dc=armijo,dc=com"
slavePw="JorgeArmijo1982"
masterDN="cn=Manager,dc=jorge,dc=armijo,dc=com"
masterPw="JorgeArmijo1982"
```

2.5 Ingreso de Información del Árbol.

2.5.1 Definición de la Organización.

La información Básica del servidor se la define en el archivo: /home/configuracion_inicial.ldif
La información que contendrá este archivo es el dominio con el cual identificaremos la organización en este caso el dominio es jorge.armijo.com y definiremos el grupo de trabajo ORGANIZACIÓN.

```
dn: dc=jorge,dc=armijo,dc=com
objectclass: dcObject
objectclass: organization
o: Tesis Jorge Armijo 2013
dc: ORGANIZACION
```

Esta información es agregada aldirectorio activo con el comando siguiente ejecutado en un terminal.

```
# slapadd -l /home/configuracion_inicial.ldif
```

2.5.2 Definición de la estructura jerárquica del árbol.

La definición de la estructura jerárquica del directorio activo se realiza con el archivo /etc/openldap/base.ldif en el cual describe el contenido de la estructura jerárquica predefinida cuando se realiza la instalación de los servicios del OpenLdap. La misma que se realiza cuando se ejecuta el siguiente comando en un terminal.

```
# ldapadd -x -W -c -D "cn=Manager,dc=jorge,dc=armijo,dc=com" -f
/etc/openldap/base.ldif
Enter LDAP Password:
```

La salida del comando anterior en terminal tendrá el siguiente aspecto:

```
adding new entry "dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Hosts,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Rpc,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Services,dc=jorge,dc=armijo,dc=com"
adding new entry "nisMapName=netgroup.byuser,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Mounts,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Networks,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=People,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Group,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Netgroup,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Protocols,dc=jorge,dc=armijo,dc=com"
adding new entry "ou=Aliases,dc=jorge,dc=armijo,dc=com"
adding new entry "nisMapName=netgroup.byhost,dc=jorge,dc=armijo,dc=com"
```

2.5.3 Definición de Conjunto de objetos.

Nos basaremos en los esquemas de información predefinidos por el servicio de samba el cual contiene información básica de usuarios tales como:

- ***Nombre***
- ***Apellido***
- ***Nombre de usuario***
- ***Teléfono***
- ***Dirección***
- ***Fotografía***
- ***Contraseña***

Uno de los avances que hacen de los Directorios Activos la herramienta de consumo de información más ágil en una organización es el poder en modificar los esquemas de información contenida personalizando la herramienta de acuerdo a las necesidades de negocio.

2.5.4 Definición de permisos.

OpenLdap nos permite tener varios niveles de seguridad para la administración de la información del directorio activo.

En este caso configuraremos tres tipos de Usuarios:

2.5.4.1 Usuarios Super Administradores.

Característica principal modificación global del directorio activo.

2.5.4.2 Usuarios Administradores.

Característica principal modificación parcial del directorio activo.

2.5.4.3 Usuarios Normales.

Característica principal consume información del directorio activo.

Estos roles son asignados a través de la herramienta de administración phpldapadmin.

2.6 Instalación y Configuración Herramientas Administración LDAP.

2.6.1 Consideraciones previas a la instalación.

Para la instalación y configuración de la herramienta de administración de Phpldapadmin necesitamos:

2.6.1.1 Versión del Sistema Operativo.

Para determinar la versión del sistema operativo ejecutamos en el terminal:

```
# cat /etc/redhat-release
```

El resultado debe ser algo similar a lo siguiente.

```
Red Hat Enterprise Linux Server release 6.4 (Santiago)Red Hat Enterprise Linux Server
```

2.6.1.2 Versión OpenLdap.

En el terminal ejecutamos:

```
# rpm -qa | grep ldap
```

Se tendrá una salida similar a la siguiente listando los paquetes instalados de OpenLdap:

```
nss-pam-ldapd-0.7.5-18.el6.x86_64
openldap-2.4.23-31.el6.x86_64
openldap-servers-2.4.23-31.el6.x86_64
smbldap-tools-0.9.5-2.el6.rf.noarch
python-ldap-2.3.10-1.el6.x86_64
pam_ldap-185-11.el6.x86_64
openldap-clients-2.4.23-31.el6.x86_64
```

2.6.1.3 Versión Samba

En el terminal ejecutamos:

```
# rpm -qa | grep samba
```

Tendremos una salida similar a la siguiente:

```
samba-winbind-clients-3.6.9-151.el6.x86_64
samba-common-3.6.9-151.el6.x86_64
samba-winbind-3.6.9-151.el6.x86_64
samba-client-3.6.9-151.el6.x86_64
samba-3.6.9-151.el6.x86_64
```

2.6.2 Instalación Phpldapadmin.

La herramienta de administración de OpenLdap "PhpLdapAdmin" está disponible de los repositorios de epel el cual ya se encuentra configurado.

2.6.3 Instalación y configuración del Servidor Web.

Para la instalación de phpldapadmin en un terminal ejecutar:

```
# yum –y install httpd
```

Instalará el paquete de httpd y sus dependencias, tendremos una salida similar a la siguiente:

```
================================================================================ Package
Arch              Version                 Repository          Size
================================================================================
Installing:
 httpd            x86_64          2.2.15-26.el6           base           821 k
Installing for dependencies:
 apr              x86_64          1.3.9-5.el6_2           base           123 k
 apr-util         x86_64          1.3.9-3.el6_0.1         base            87 k
 apr-util-ldap    x86_64          1.3.9-3.el6_0.1         base            15 k
 httpd-tools      x86_64          2.2.15-26.el6           base            72 k

Transaction Summary
================================================================================Install
5 Package(s)
```

2.6.4 Instalación y Configuración del PhpLdapAdmin.

En un terminal ejecutar:

```
# yum –y install phpldapadmin
```

Instalará el paquete de Phpldapadmin y sus dependencias, tendremos una salida similar a la siguiente:

```
================================================================================
 Package                Arch              Version                 Repository        Size
================================================================================
Installing:
 phpldapadmin           noarch            1.2.3-1.el6             epel              806 k
Installing for dependencies:
 apr                    x86_64            1.3.9-5.el6_2           base              123 k
 apr-util               x86_64            1.3.9-3.el6_0.1         base               87 k
 apr-util-ldap          x86_64            1.3.9-3.el6_0.1         base               15 k
 lighttpd               x86_64            1.4.32-1.el6            epel              291 k
 php                    x86_64            5.3.3-22.el6            base              1.1 M
 php-cli                x86_64            5.3.3-22.el6            base              2.2 M
 php-common             x86_64            5.3.3-22.el6            base              524 k
 php-ldap               x86_64            5.3.3-22.el6            base               38 k

Transaction Summary
================================================================================
Install      9 Package(s)
```

Configuración del Phpldapadmin para acceder al directorio activo.

Se debe editar el archivo /etc/httpd/conf.d/php.conf y se debe reemplazar las siguientes líneas:

```
<Directory /usr/share/phpldapadmin/htdocs>
  Order Allow,Deny
  Allow from all
  Allow from 127.0.0.1
  Allow from ::1
```

Con esta modificación se permitirá el acceso desde cualquier dirección IP del mismo segmento de red a la herramienta del phpldapadmin.

Editaremos el archivo /usr/share/phpldapadmin/config/config.php las siguientes líneas:

```
$servers->setValue('server','name','Cluster LDAP Server Jorge Armijo');
$servers->setValue('server','host','192.168.12.20');
```

Donde se indicara el nombre que aparecerá en la cabecera del directorio activo y la dirección IP a la cual deberá direccionarse la herramienta para realizar la búsqueda del directorio activo OpenLdap.

```
$servers->setValue('server','name','Cluster LDAP Server Jorge Armijo');
$servers->setValue('server','host','192.168.12.20');
```

La dirección IP 192.168.12.20 corresponde a la dirección IP flotante que se configurara para la habilitación del clúster.

2.7 Instalación de un sistema de Alta disponibilidad.

2.7.1 Compatibilidad de Versiones Software a Instalar.

Al proveer paquetes directamente del DVD de Instalación de RHEL estas son las ultimas estables y con las cuales se desarrolló esta guía metodológica.

2.7.2 Instalación Sistema de Alta Disponibilidad.

En un terminal ejecutar:

```
# yum groupinstall -y “High Availability”
```

2.7.3 Instalación Sistema de almacenamiento compartido.

En un terminal ejecutar:

```
# yum groupinstall -y “Resilient Storage”
```

2.7.4 Instalación de paquetes para la administración de fencing.

En un terminal ejecutar:

```
# yum install -y fence-virt fence-virtd fence-virtd-libvirt fence-virtd-multicast fence-virtd-serial fence-agents fence-virtd-checkpoint
```

2.7.5 Configuración Sistema de Alta Disponibilidad.

2.7.5.1 Configuración del Administrador del Clúster.

En el terminal ejecutar:

```
# yum install luci
```

Luci es el demonio para la consola de administración de Clúster de Red Hat.

Habilitamos los demonios del clúster al inicio de los servidores.

```
# chkconfig luci on
# chkconfig cman on
# chkconfig rgmanager on
# chkconfig modclusterd on
# chkconfig clvmd on
```

2.7.5.2 Configuración de Nodos del Clúster.

Ricci es el demonio para los nodos que conforman el Clúster de Red Hat.

Habilitamos los demonios del clúster al inicio de los servidores.

```
# chkconfig ricci on
# chkconfig cman on
# chkconfig rgmanager on
# chkconfig modclusterd on
# chkconfig clvmd on
```

2.7.6 Configuración del servidor LDAP-SAMBA en alta disponibilidad.

2.7.6.1 Definición de las direcciones y hosts que intervendrán en el entorno de Alta Disponibilidad.

Nodo	Dirección IP	hostname	Rol
0	192.168.12.10	clsterm.jorgearmijo.com	Administrador
1	192.168.12.1	clster1.jorgearmijo.com	Nodo cluster1
2	192.168.12.2	clster2.jorgearmijo.com	Nodo cluster2
3	192.168.12.3	clster3.jorgearmijo.com	Nodo cluster3
4	192.168.12.4	clster4.jorgearmijo.com	Nodo cluster4

Tabla 5.1 Direccionamiento IP servidores clúster.

2.7.6.2 Ingreso a la consola de administración de clúster.

Para el ingreso a la consola de administración en un navegador escribir la dirección:

```
https://192.168.12.10:8084/
```

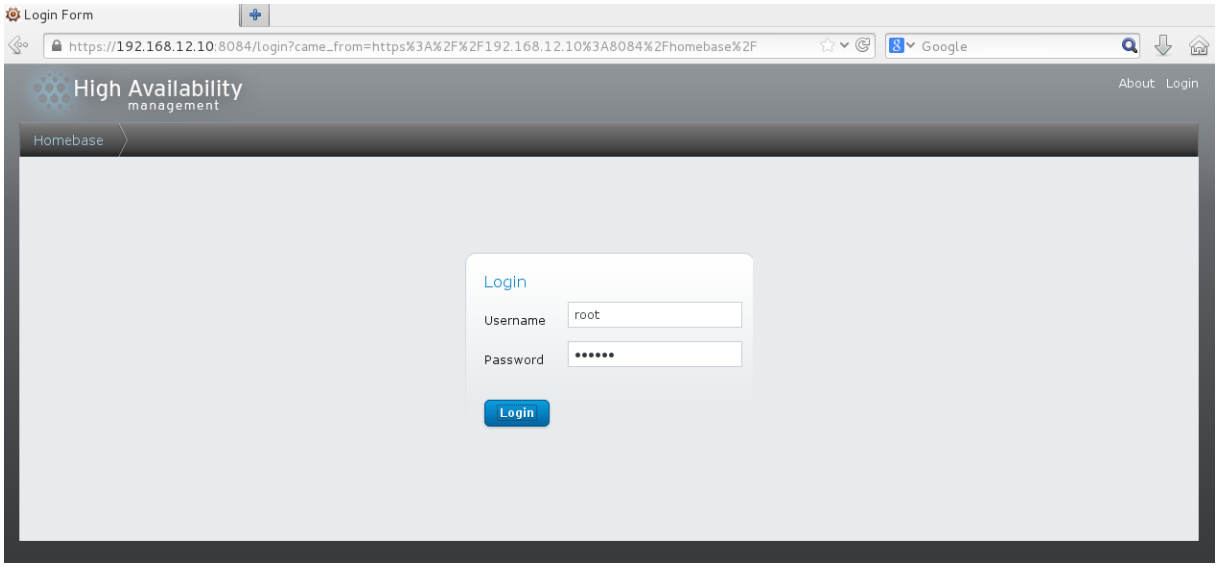
2.7.6.3 Creación de un clúster.

Se presentará la Imagen de ingreso al administrador del Clúster

Digitar el usuario y contraseña:

Usuario: root

Contraseña: redhat)

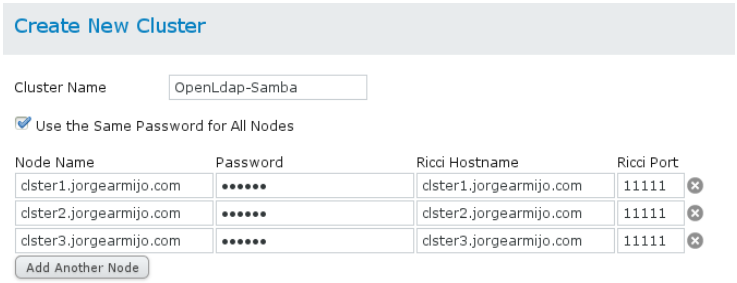


2.7.6.4 Creación de un clúster

Para la creación del clúster se debe tener configurados los hosts en un DNS de manera que el administrador del clúster pueda resolver los hostname y las direcciones IP para cada nodo que intervendrán en el clúster.

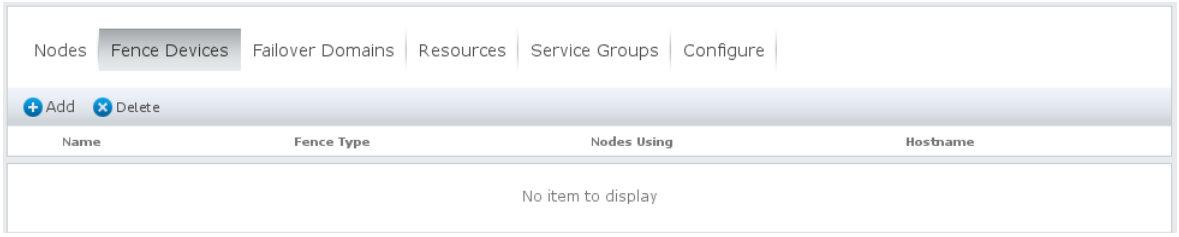
Para la creación del clúster seleccionar del menú principal “Create”

Donde solicitara el ingreso del nombre del clúster así como el de los hosts y la contraseña del agente del entorno de virtualización ricci.

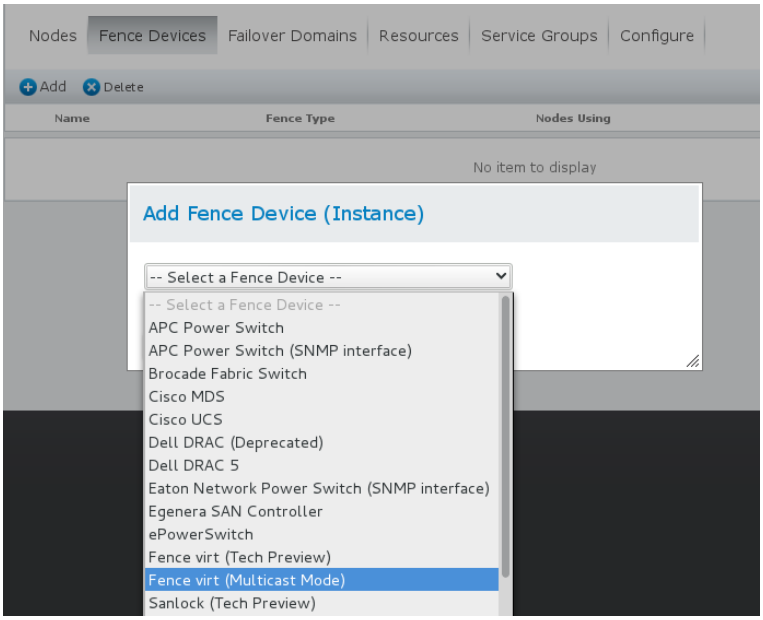


2.7.6.5 Definición de un dispositivo de fencing.

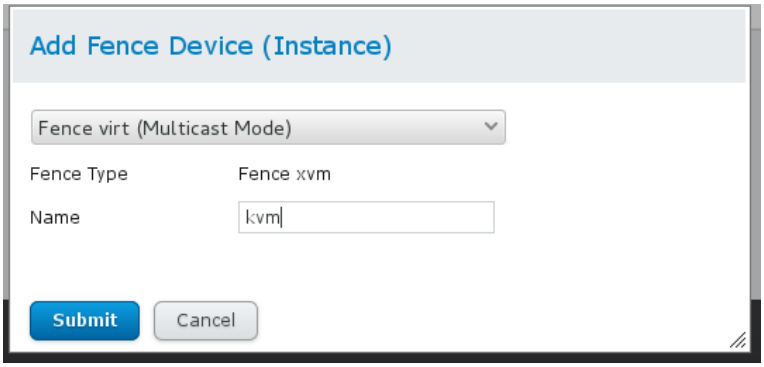
Un dispositivo de fencing será definido dependiendo de la tecnología de Hardware que se disponga. Para el desarrollo de esta guía metodológica se utilizara el virtualizador KVM.



En el menú de Fence Devices seleccionamos “agregar” y seleccionamos de la lista “Fence virt (Multicast Mode)”



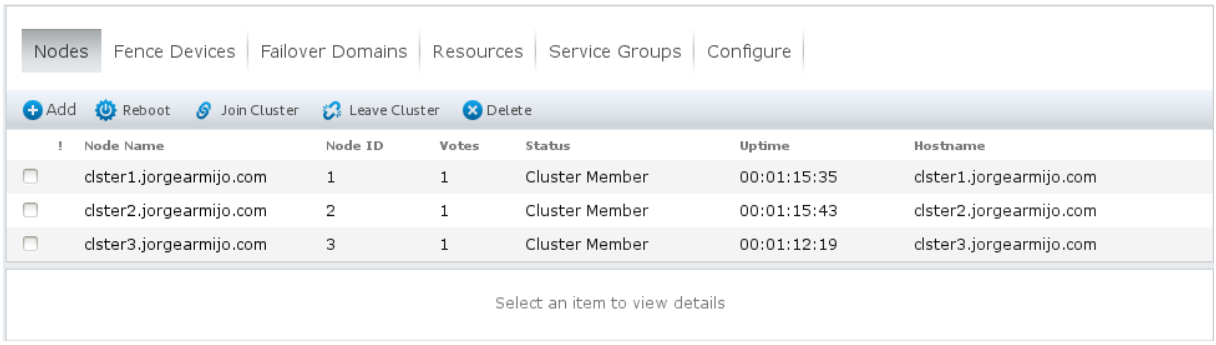
Seleccionamos un nombre que nos sea fácil de identificar el tipo de Fencing a usar este caso “kvm”



2.7.6.6 Definición de métodos de fencing para cada nodo del clúster.

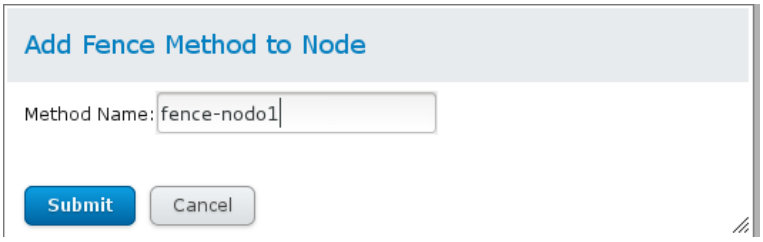
Una vez definido el método de fencing se lo debe de configurar en cada nodo del clúster de la siguiente forma.

En el menú de nodos del clúster se debe realizar la siguiente configuración para cada uno de los nodos.

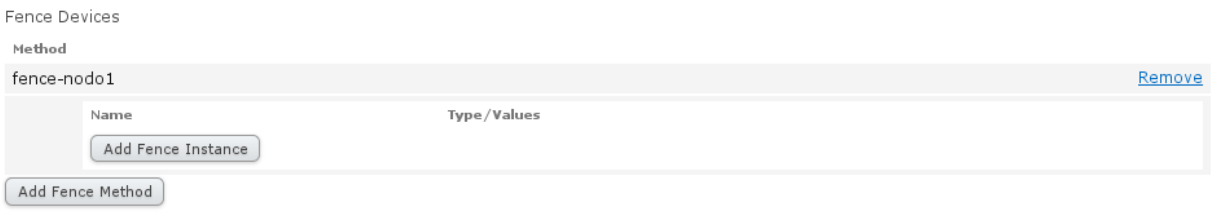


Seleccionar el nodo clster1.jorgearmijo.com agregar un método de fencing.

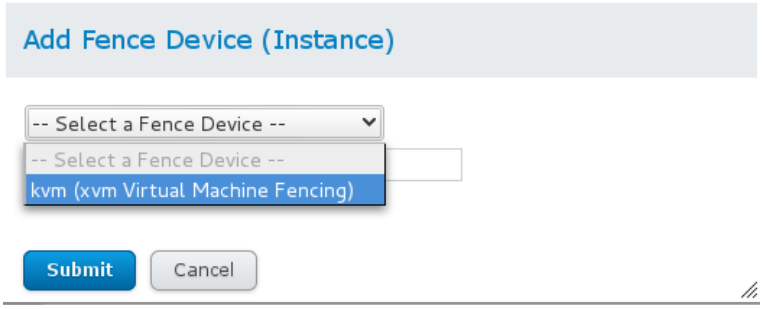
Se escogerá un nombre que pueda ser fácil de identificar para el fencing de este nodo.



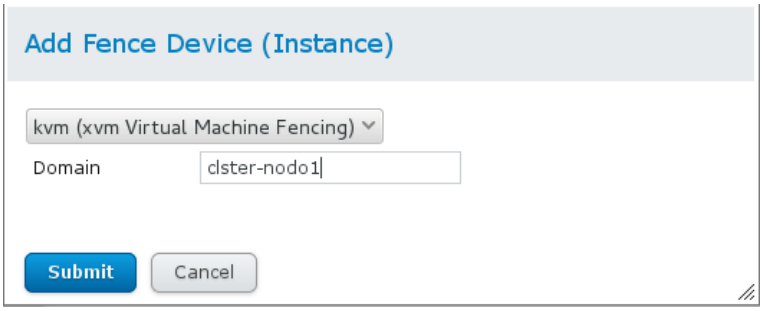
Posterior a esto se debe definir una instancia del fencing.



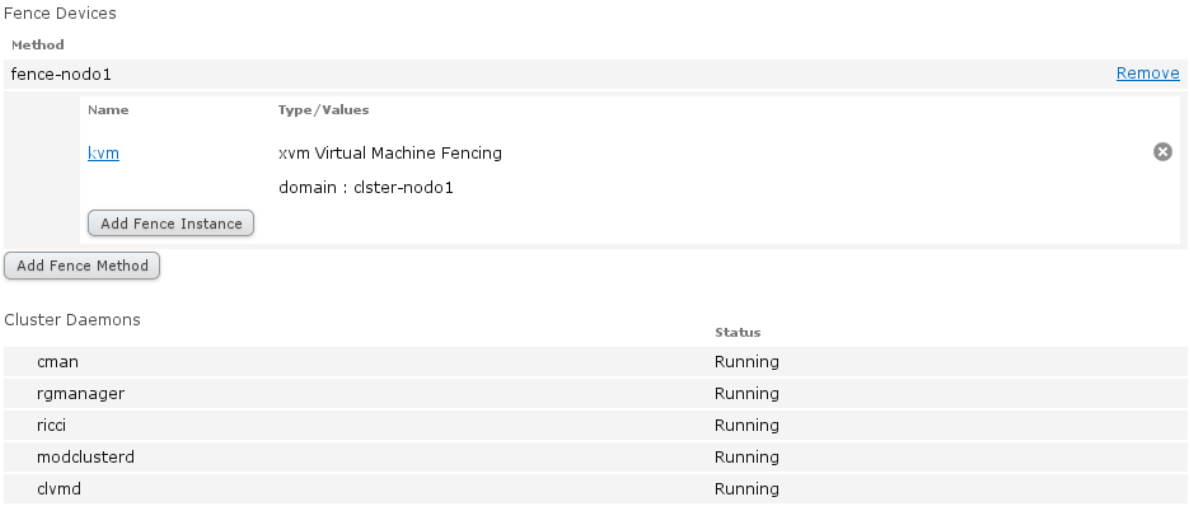
Se seleccionará el dispositivo de fencing configurado y se identificara con el nombre del host definido en el entorno del virtualizador KVM “clster-nodo1”.



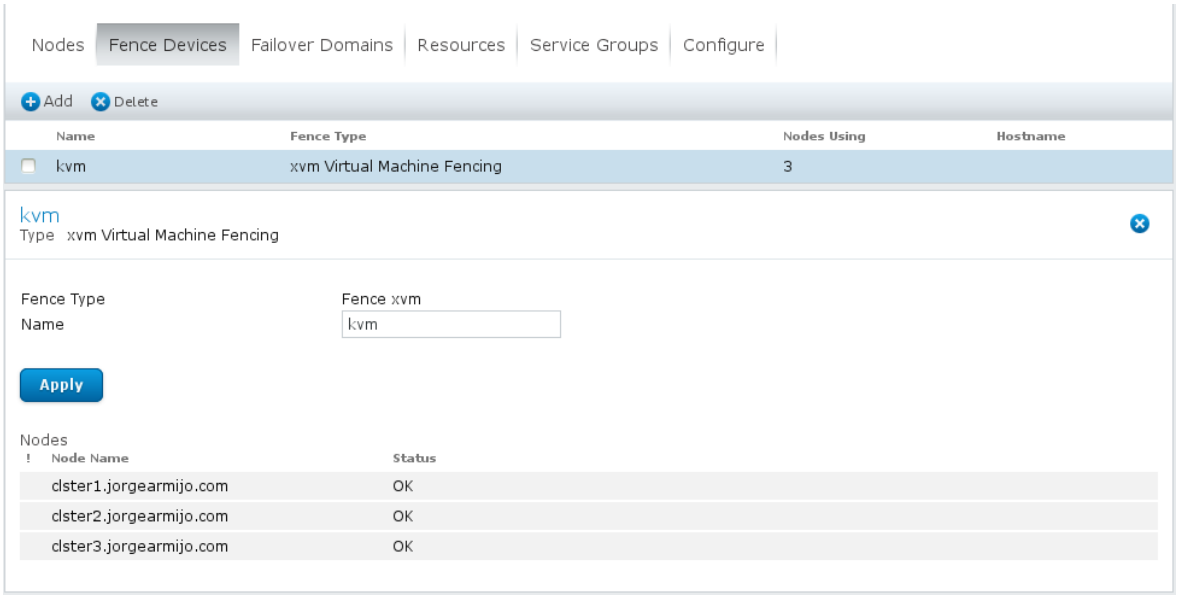
Se obtendrá algo similar a lo siguiente.



Detalle de la configuración del fencing y de los demonios que deben estar activos en cada nodo del clúster.

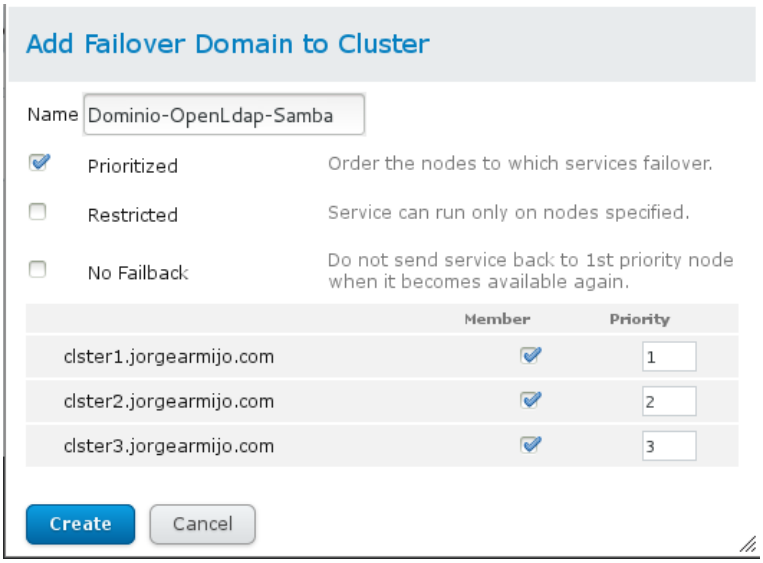


Una vez definido los métodos de fencing para cada nodo se debe proceder a tener en el menú del fenece device algo similar a lo siguiente.



2.7.6.7 Definición de un Dominio de cluster.

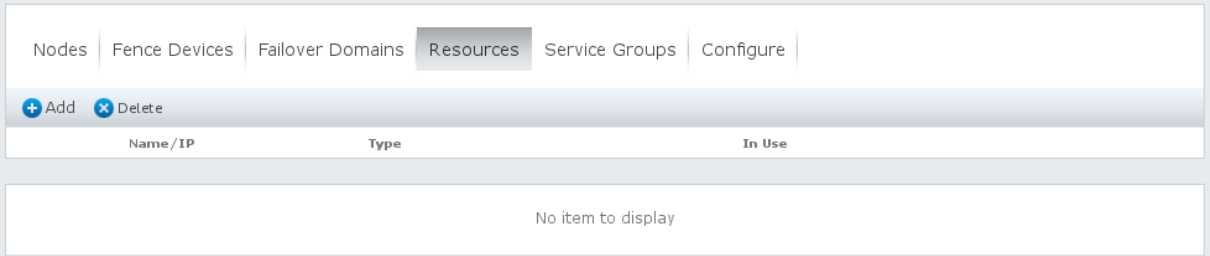
Un dominio de servicios consiste en el listado de los servidores "nodos" que se configuraran en el clúster y la prioridad con la cual se definirá a cada uno de ellos en el clúster "OpenLdap-Samba". Para este caso en particular se definirán los tres nodos establecidos previamente.



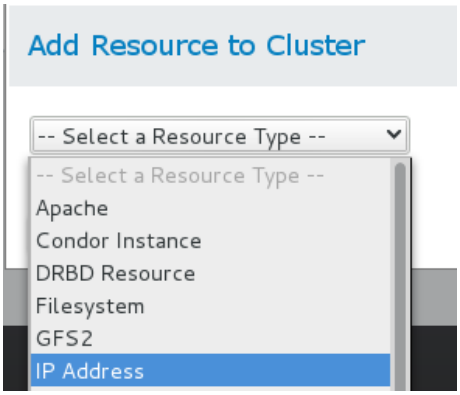
Se debe otorgar la prioridad a uno de los nodos para identificar el orden de prioridad en levantar los servicios definidos en los nodos del cluster.

2.7.6.8 Definición de servicios del clúster.

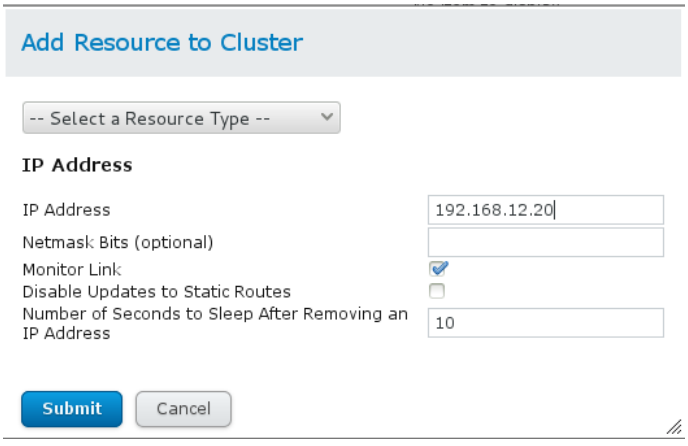
Dentro del menú de “Resources” se procederá a la definición de servicios para el clusrter.



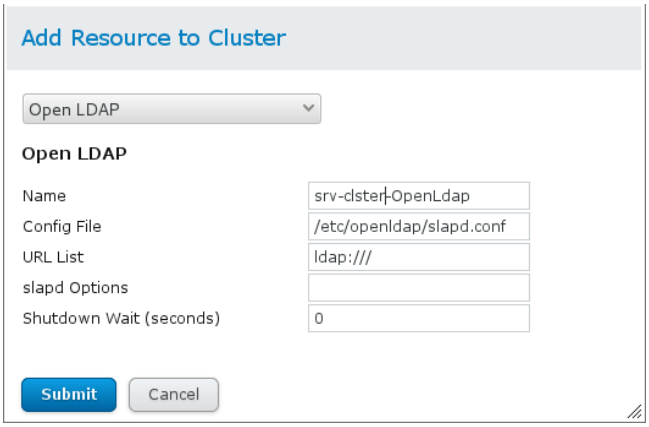
Se debe escoger de la lista el servicio a configurar uno de los servicios del clúster en este ejemplo IP Address que se convertirá en la configuración para la dirección IP flotante del cluster.



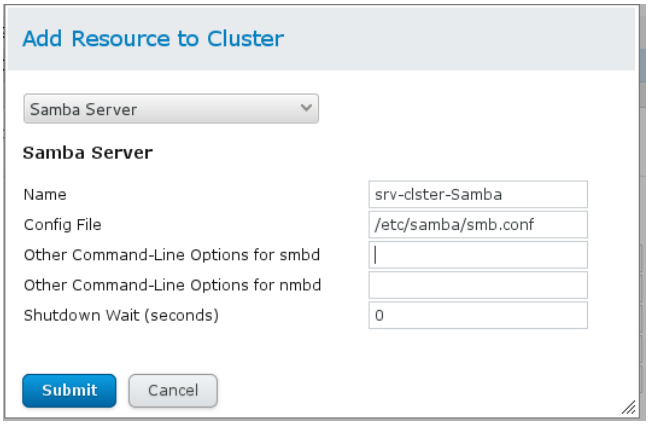
Para realización del Clúster Activo-Pasivo de los servicios de OpenLdap y Samba definidos para el desarrollo de esta guía metodológica se necesita configurar una dirección IP “flotante” la cual nos permitirá acceder a los servicios del clúster definidos.



Para el servicio del OpenLdap se procederá de la misma forma pero se seleccionará OpenLdap del listado presentado.

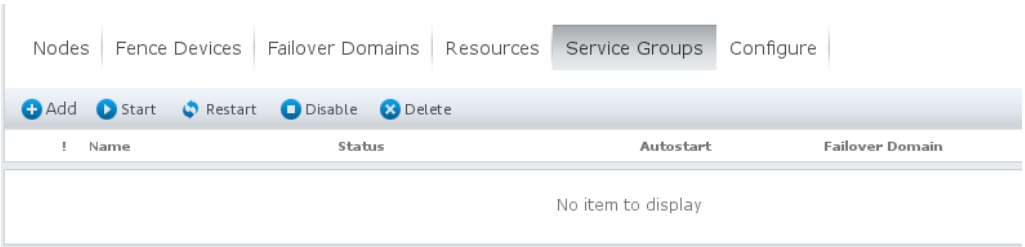


Para el servicio del Samba procederemos de la misma forma pero se escogera Samba del listado presentado.

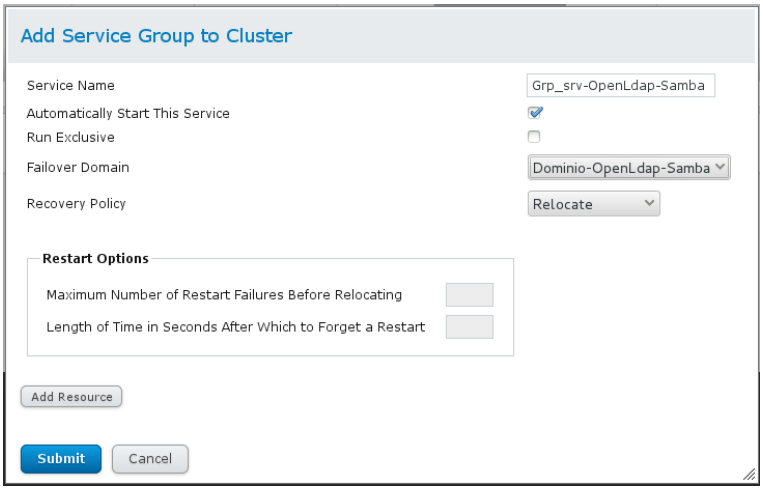


2.7.6.9 Definición de grupos de servicios.

La definición de servicios nos permitirá configurar el comportamiento de los servicios del clúster.



En el menú de “Service Groups” seleccionaremos el nombre del Grupo y los servicios que serán definidos en este grupo.



En este Grupo de servicios se definirá:

Que el grupo de servicios inicie automáticamente cuando se enciendan los nodos.

Domino que levantara los servicios definidos.

Política de recuperación cuando un nodo falla.

2.8 Configuración de sistemas operativos para la integración con el LDAP-SAMBA.

2.8.1 Configuración de sistemas operativos de código abierto.

2.8.1.1 Configuración de red.

Nodo	Dirección IP	hostname	Distribución
1	192.168.12.40	workstation.jorgearmijo.com	Redhat-workstation
2	192.168.12.41	fedora.jorgearmijo.com	Fedora

Tabla5.2.1 Direccionamiento clientes Linux

Para la Configuración del hostname editar el archivo /etc/hosts y agregar la siguiente linea:

```
192.168.12.40 workstation.jorgearmijo.com workstation
```

2.8.1.2 Configuración de credenciales de autenticidad.

Para configurar las credenciales de autenticidad ejecutaremos la herramienta authconfig-gtk donde definiremos los siguientes parámetros:

- Dirección IP del clúster del LDAP (192.168.12.20).
- Base de Búsqueda del LDAP.
- Certificado de Autenticidad.
- Tipo de contraseña a usar.
- Crear directorio al iniciar sesión de usuario.

Descarga del certificado de Autenticidad

Una vez definidos estos parámetros se puede a añadir en el archivo /etc/sssd/sssd.conf la siguiente línea que nos permite realizar la conexión de equipos al dominio definido.

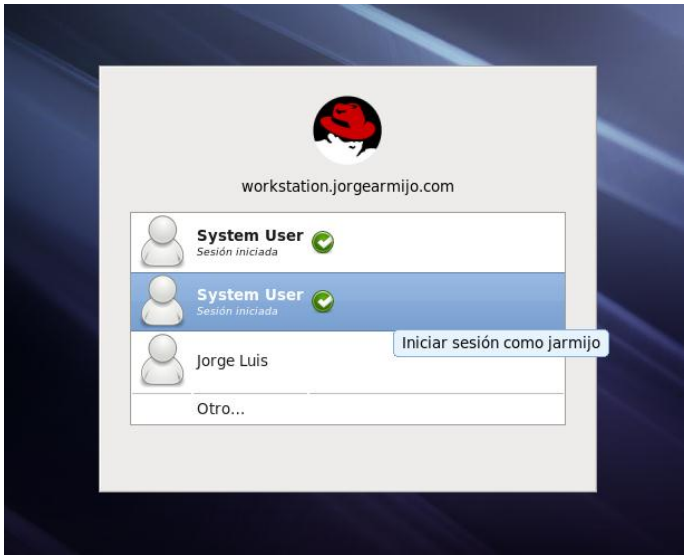
```
enumerate = True
```

Para validar las cuentas de usuario ejecutamos en el terminal:

```
# getent passwd
apantoja:*:50012:513:System User:/home/apantoja:/bin/sh
asalazar:*:58376:544:System User:/home/asalazar:/bin/sh
dcordova:*:49118:544:System User:/home/dcordova:/bin/sh
mmoreira:*:3723:513:System User:/home/mmoreira:/bin/sh
ppantoja:*:57424:513:System User:/home/ppantoja:/bin/sh
jarmijo:*:1850:544:System User:/home/jarmijo:/bin/sh
karmijo:*:32063:513:System User:/home/karmijo:/bin/sh
berazo:*:45296:513:System User:/home/berazo:/bin/sh
bquito:*:63311:513:System User:/home/bquito:/bin/sh
jquito:*:13175:513:System User:/home/jquito:/bin/sh
mquito:*:17717:513:System User:/home/mquito:/bin/sh
vparra:*:39848:513:System User:/home/vparra:/bin/bash
```

Se puede observar los usuarios que pertenecen al OpenLdap ya que describe un número alto en el en UID y en el GID el 513 correspondiente a los Domain Users.

Desde la pantalla de ingreso de sesión se puede ingresar con el Usuario de Dominio jarmijo.



Esta configuración realizada es compatible con versiones de fedora 18 fedora 19 fedora 20. Ya que están basados en el kernel del RHEL como su distribución de OpenSource definida.

2.8.2 Configuración de sistemas operativos Licenciados.

2.8.2.1 Configuración de red.

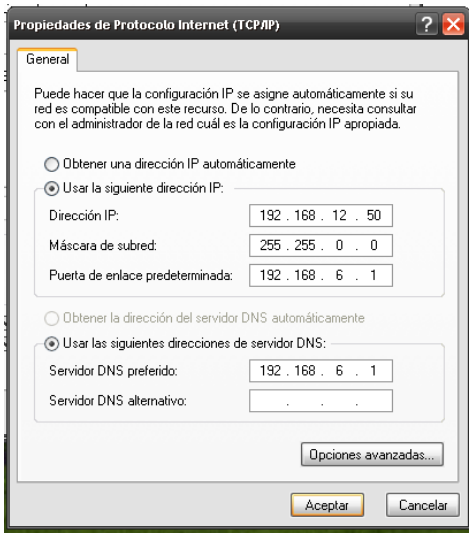
Nodo	Dirección IP	hostname	Distribución
0	192.168.12.50	win_xp.jorgearmijo.com	Windows XP
1	192.168.12.51	win_7.jorgearmijo.com	Windows 7
2	192.168.12.52	win_8.jorgearmijo.com	Windows 8

Tabla5.2.2 Direccionamiento clientes Windows

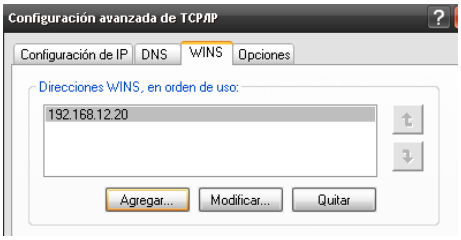
2.8.2.2 Configuración Windows XP.

Editar las conexiones de área local.

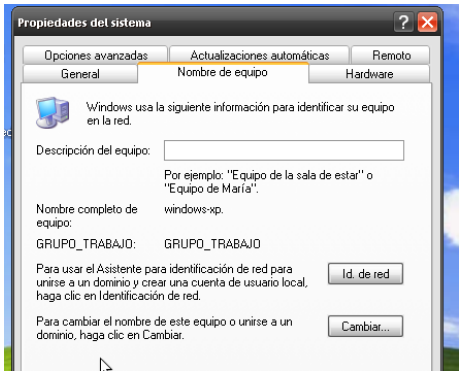
Editar las propiedades 4(TCP/IP)



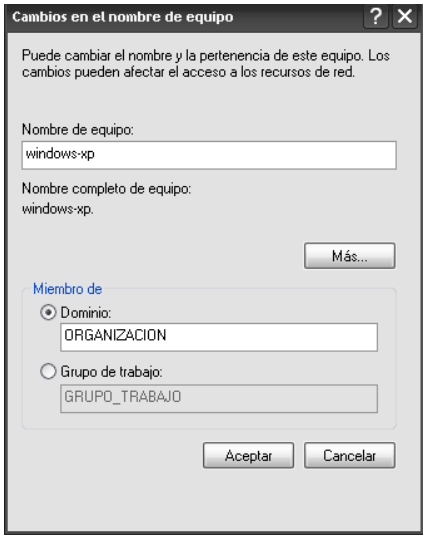
En opciones avanzadas seleccionamos la pestaña de WINS y agregamos la IP del clúster (192.168.12.20).



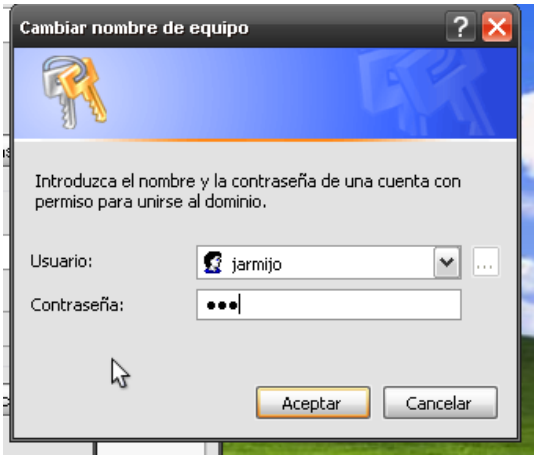
Para ingresar un equipo en el Dominio debemos cambiar el nombre del Grupo de trabajo por el definido en los archivos del samba el mismo que es "ORGANIZACION".



Se debe seleccionar el botón ***"cambiar"*** y se presentara la pantalla para ingresar el nombre del dominio. En este caso "ORGANIZACION"



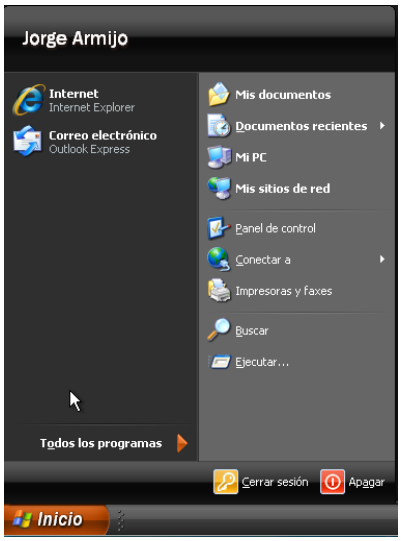
Se ingresa una cuenta de Usuario Administrador del Dominio para unir el equipo.



A continuación se presentara el mensaje de que el equipo ha sido unido correctamente al dominio y nos pedirá reiniciar el equipo.

Ingresar con una cuenta de usuario y se podrá configurar el escritorio para cada uno de los usuarios registrados en el domino.

Como se observa una vez iniciada la sesión muestra el Nombre del Usuario “Jorge Armijo” registrado en el OpenLdap.



2.8.2.3 Configuración para Windows 7 y Windows 8

Para Ingresar Equipos Windows 7 y 8 se debe realizar una modificación en el registro de Windows para que permita conectarse al Dominio Open Ldap + Samba.

Se debe guardar esta configuración en un archivo regedit y se deberá reiniciar el equipo para que sean efectivos los cambios.

El contenido para la modificación de parámetros del registro de Windows es el siguiente:

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters]
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001
"EnableSecuritySignature"=dword:00000000

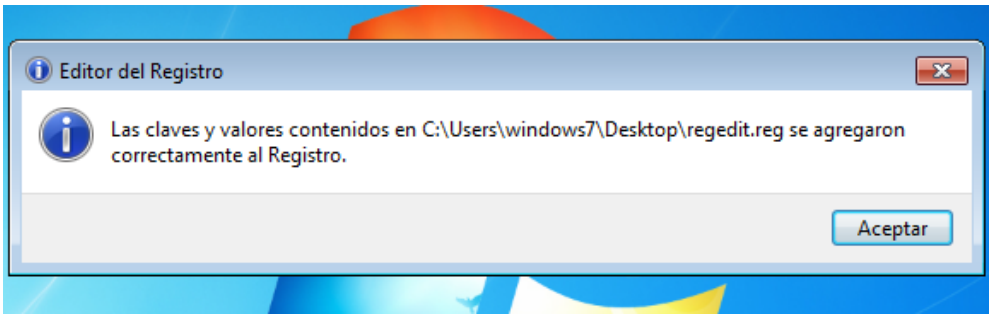
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Netlogon\Parameters]
"RequireSignOrSeal"=dword:00000001
"RequireStrongKey"=dword:00000001
"SealSecureChannel"=dword:00000001
"SignSecureChannel"=dword:00000001

El contenido para la modificación de parámetros del registro de Windows es el siguiente:

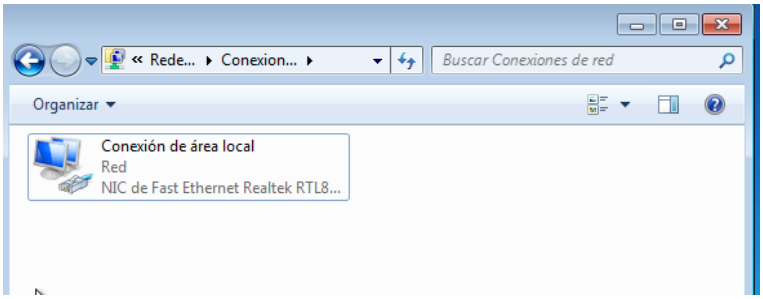
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters]
"QualifyingDestinationThreshold"=dword:00000003
"NV Domain"="ORGANIZACION"
"NameServer"="ORGANIZACION"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\System\DNSClient]
"NV PrimaryDnsSuffix"=" ORGANIZACION "
```

Estas configuraciones se las debe de guardar en un archivo de texto como ***"modificación_registro.reg"*** para facilitar la modificación del registro de Windows.

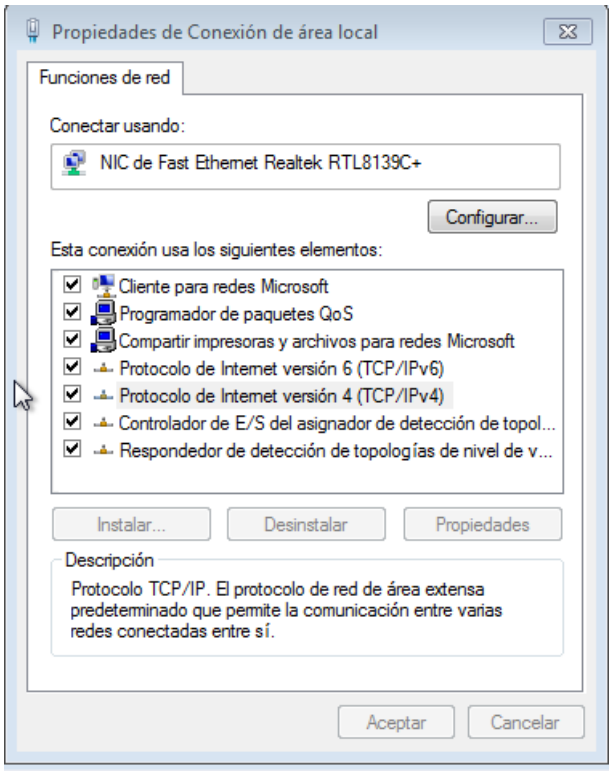
Una vez creado el archivo se debe proceder a ejecutarlo y reiniciar el equipo como lo muestra esta guía.



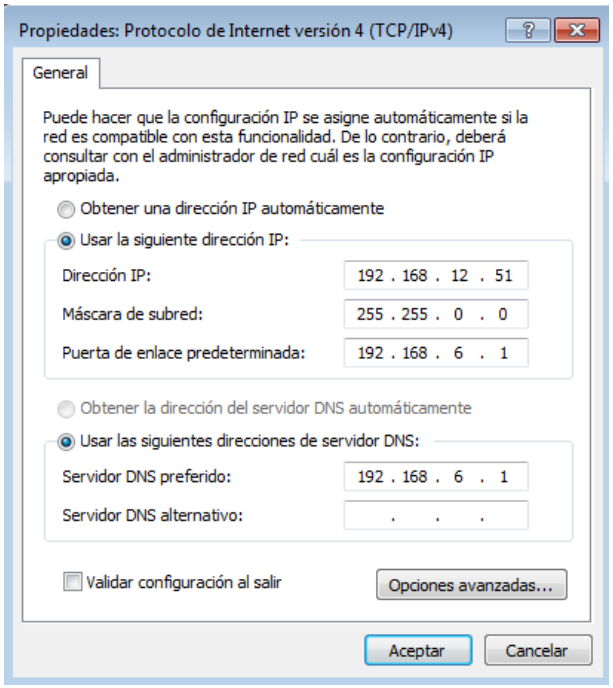
Una vez reiniciado el equipo se debe editar las conexiones de área local para agregar como servidor ***"wins"*** la IP del cluster.



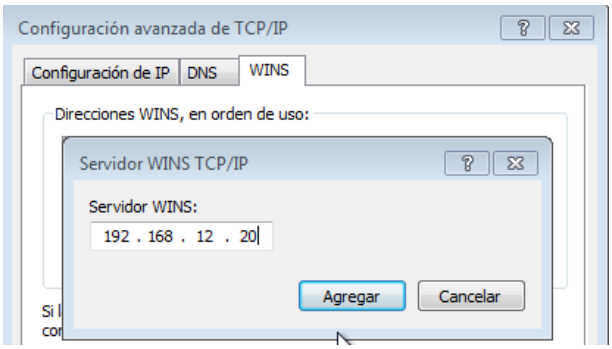
Editar las propiedades 4(TCP/IP)



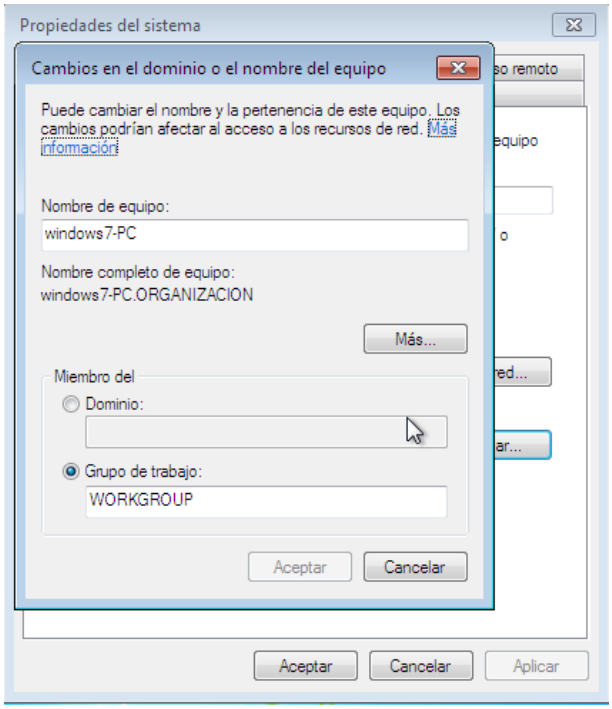
Definir el direccionamiento IP



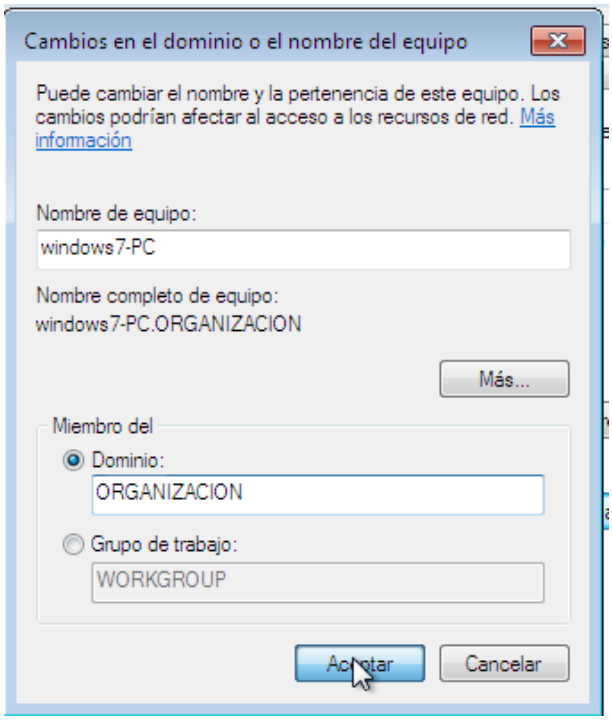
En opciones avanzadas seleccionamos la pestaña de WINS se debe indicar la dirección IP del definida para el Clúster del OpenLdap + Samba.



Para ingresar un equipo en el Dominio se debe de modificar el nombre del ***"Grupo de trabajo"*** por el definido en los archivos del samba el mismo que es ***"ORGANIZACION".***

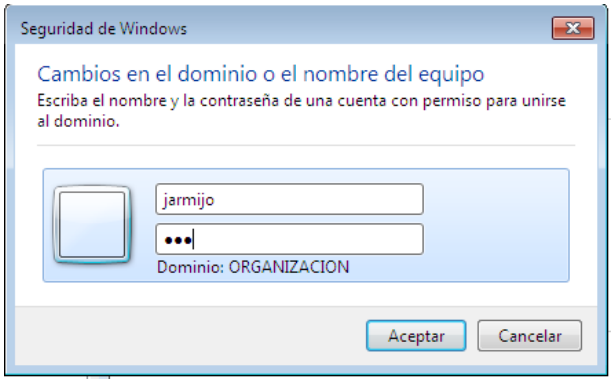


Se debe seleccionar el botón de ***"Cambiar"*** y se presentara la pantalla para ingresar el nombre del dominio. En este caso ***"ORGANIZACION"***



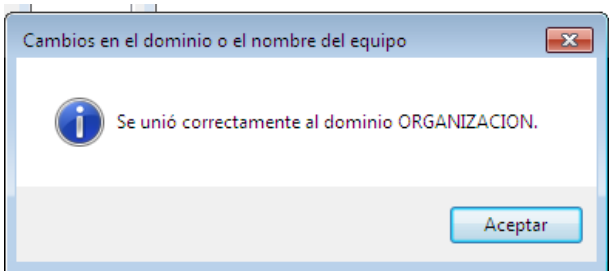
Al realizar este procedimiento nos presentara una pantalla para ingresar una cuenta de Usuario Administrador definida en el Dominio para unir el equipo al mismo.

En este caso jarmijo esta asignado como usuario administrador en el Directorio Activo.

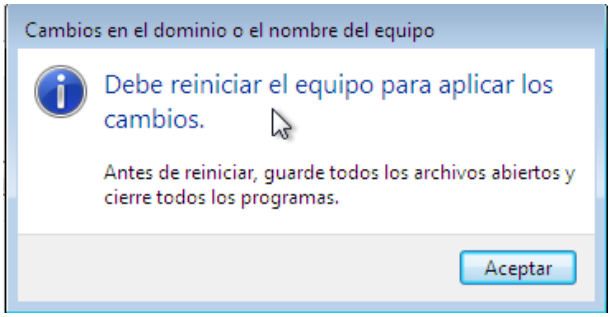


Una ver realizado esto el equipo validará las configuraciones definidas para el Servidor de Dominio

Una vez validadas las configuración se presentará el mensaje de que el equipo ha sido unido correctamente al dominio y nos pedirá reiniciar el equipo.

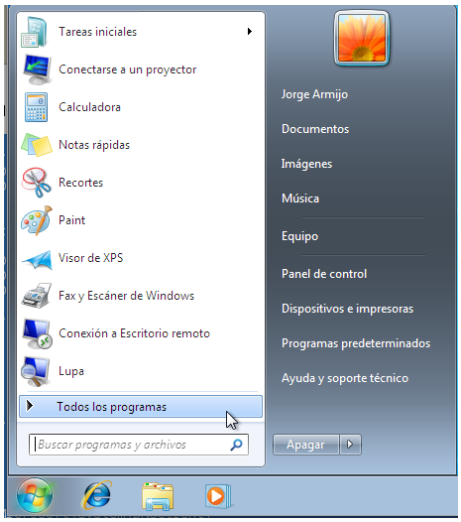


Se debe de reiniciar el equipo para que los cambios de ingreso al domino sean efectivos.



Una vez reiniciado el equipo se puede ya ingresar al dominio con una cuenta de usuario definida en el Directorio Activo.

Como se observa una vez dentro del dominio el Nombre del Usuario del OpenLdap “Jorge Armijo” se muestra en el inicio de la sesión



Nota: Los mismos procedimientos se deben de realizar para unir un equipo con Windows 8

CAPITULO 3

3. Validación de la Guía metodológica para la implementación de un Protocolo Ligero de Acceso a Directorios con un Controlador de Dominio Principal en un entorno de Alta disponibilidad.

Para la validación de esta guía metodológica se ha desarrollado un script de instalación y configuración de OpenLdap y Samba adicionalmente de las configuraciones necesarias del sistema operativo para el funcionamiento de un entorno de alta disponibilidad

Estos scripts se encuentran desarrollados en el lenguaje de programación Shell de Linux, están basados en las configuraciones establecidas en el capítulo dos de esta guía metodológica.

Para la validación de esta guía los scripts están divididos en secciones como:

- Configuración hostname del equipo.
- Configuración del repositorio local de paquetes.
- Instalación y configuración OpenLdap.
- Instalación y Configuración de Samba.
- Instalación y Configuración de Phpldapadmin.
- Instalación de Webmin.
- Configuración del firewall.
- Configuración de paquetes para Alta Disponibilidad.

3.1 Instalación y configuración del sistema operativo RHEL6.5

Para la validación de la versión del Sistema Operativo y configuraciones extras para el entorno de alta disponibilidad se utilizara los scripts de configuración llamados:

- Configuración hostname del equipo.
- Configuración del repositorio local de paquetes.
- Configuración del firewall.

Para validar la versión del sistema Operativo:

```
# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 6.5 (Santiago)
```

Este comando determina la versión del sistema Operativo que se está utilizando así como el nombre que ha sido asignado a esta distribución.

3.1.1 Configuración hostname del equipo.

Para realizar la validación del hostname del equipo ejecutaremos el script llamado "configurar_hostname.sh", cuyo contenido es el siguiente.

```
#!/bin/sh
clear
echo "            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "               DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "                 CONFIGURACIÓN DE HOSTNAME"
echo
"============================================================
======"
#echo "Si es una instalación nueva escriba "nodo" caso contrario hostname actual"
echo "Ingrese Hostname (en minusculas y sin dominio, ejm: clster1):"
#read
actual="nodo"
echo "Ingrese Hostname Nuevo:"
read nuevo
echo "Ingrese la Dirección IP"
read ip
raiz="/OpenLdap_Samba_HA/configuraciones"
mv /etc/sysconfig/network /etc/sysconfig/network.bk
cp $raiz/network /etc/sysconfig/network
sed "s/nodo/$nuevo/g" $raiz/hosts > /etc/hosts
mv /etc/hosts /etc/hosts.bk
sed "s/dir_ip/$ip/g" /etc/hosts.bk > /etc/hosts
hostname $nuevo.jorgearmijo.com

[ $actual = "nodo" ] &&
sed "s/localhost.localdomain/$nuevo/g" /etc/sysconfig/network > $raiz/network.1 ||
sed "s/$actual/$nuevo/g" /etc/sysconfig/network > $raiz/network.1

[ $actual = "nodo" ] &&
sed "s/nodo/$nuevo/g" /etc/sysconfig/network > $raiz/network.1 ||
sed "s/$actual/$nuevo/g" /etc/sysconfig/network > $raiz/network.1
mv $raiz/network.1 /etc/sysconfig/network
echo "El servidor se reiniciara "
reboot
```

3.1.2 Configuración del repositorio local de paquetes.

Para realizar la validación del repositorio de paquetes del equipo ejecutaremos el script llamado “configurar_localrepo.sh” cuyo contenido es el siguiente.

```
#!/bin/sh
clear
echo "            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "              DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "               CONFIGURACIÓN REPOSITORIO LOCAL"
echo
"============================================================="
echo "Debe estar colocado el DVD"
raiz="/OpenLdap_Samba_HA/configuraciones"
cp -r $raiz/local.repo /etc/yum.repos.d/
mkdir /media/rhel
umount /media/RHE*
mount /dev/cdrom /media/rhel
yum repolist
```

Para validar la disponibilidad de paquetes de software ejecutar en un terminal:

```
# yum repolist
```

El comando desplegará una salida similar a la siguiente:

```
Loaded plugins: product-id, security, subscription-manager
This system is not registered to Red Hat Subscription Management. You can use
subscription-manager to register.
repo id                 repo name               status
HighAvailability        HighAvailability        56
LoadBalancer            LoadBalancer            4
ResilientStorage        ResilientStorage        62
ScalableFileSystem      ResilientStorage        7
base                    Local                   3.648
epel_local              Repo local de Epel      12
repolist: 3.789
```

Este comando sirve para listar los canales de software disponible y la cantidad de paquetes que están incluidos en cada uno de ellos.

3.1.3 Configuración del firewall.

Para realizar la validación del firewall del equipo ejecutaremos el script llamado "configurar_iptables.sh" cuyo contenido es el siguiente:

```
#!/bin/sh
clear
echo "        PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "           DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "               CONFIGURACIÓN IPTABLES"
echo "============================================================"
raiz="/OpenLdap_Samba_HA/configuraciones"
cp -f $raiz/iptables /etc/sysconfig/iptables
cp -f $raiz/iptables-config /etc/sysconfig/iptables-config
/etc/init.d/iptables start
/etc/init.d/iptables restart
/etc/init.d/iptables save
chkconfig iptables on
clear
echo "============================================================"
echo "               CONFIGURACIÓN IPTABLES"
echo "============================================================"
iptables -nvL
```

El script al finalizar deberá mostrar la configuración de los puertos que se encuentran abiertos para la comunicación con los servidores de administración del entorno de alta disponibilidad y los equipos clientes.

```
  4   240 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:22
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:137
553 43134 ACCEPT     udp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW udp dpt:137
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:138
  0     0 ACCEPT     udp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW udp dpt:138
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:139
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:445
  0     0 ACCEPT     udp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW udp dpt:445
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:389
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:636
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:80
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:8080
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:443
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:10000
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:21064
  0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:11111
  0     0 ACCEPT     udp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW udp dpt:11111
  1    60 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:16851
```

3.2 Instalación Protocolo Ligero de Acceso a Directorios (LDAP).

Para la validación de la instalación y configuración del LDAP para el entorno de alta disponibilidad se utilizará el script de configuración llamado:

- Instalador_ldap_samba_p1.sh

Para realizar la validación de la instalación y configuración de LDAP en el equipo se debe ejecutar el script llamado "Instalador_ldap_samba_p1.sh" cuyo contenido es el siguiente:

```
clear
echo"            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo"               DISERTACIÓN DE GRADO JORGE ARMIJO"
echo"                     INSTALACIÓN OPENLDAP"
echo"=============================================================================
==="
clear
raiz="/OpenLdap_Samba_HA/configuraciones"
rm -f /var/lib/ldap/*
yum -y install openldap openldap-clients openldap-servers nss-pam-ldapd
yum -y install authconfig authconfig-gtk migrationtools
yum -y install samba smbldap-tools
chcon -R -t slapd_db_t /var/lib/ldap
cp $raiz/ldap /etc/sysconfig/ldap
cp $raiz/ldap.conf /etc/openldap/ldap.conf
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chmod 700 /var/lib/ldap
chown ldap:ldap /var/lib/ldap/DB_CONFIG
cp $raiz/slapd.conf /etc/openldap/slapd.conf
echo "CONFIGURACIÓN PASSWORD ADMINISTRACIÓN LDAP"
echo "clave del ldap:\"secret\""
echo " $(slappasswd -s Jorge2013Armijo)" >/pw
while read line
do
      echo -e "$line\n"
      sed "s/secret/$line/g" $raiz/slapd.conf > /etc/openldap/slapd.conf
done < "/pw"
rm -rf /pw
chown ldap:ldap /etc/openldap/slapd.conf
chown -R ldap. /etc/openldap/slapd.d
chmod -R 700 /etc/openldap/slapd.d
chmod 600 /etc/openldap/slapd.conf
rm -rf /etc/openldap/slapd.d/*
slapadd -l $raiz/configuracion_inicial.ldif
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
chown -R ldap:ldap /var/lib/ldap
chown -R ldap:ldap /etc/openldap/slapd.d
service slapd start
```

Para la validación de la versión del Protocolo de acceso a directorios LDAP instalado en el sistema operativo se debe ejecutar en el terminal la siguiente línea.

```
# rpm -qa | grep openldap
```

Esto listará la versión instalada y configurada de las herramientas de integración de Open Ldap.

```
openldap-2.4.23-31.el6.x86_64
openldap-servers-2.4.23-31.el6.x86_64
openldap-clients-2.4.23-31.el6.x86_64
```

Para validar la instalación y configuración de las herramientas de integración de Open Ldap y Samba se debe ejecutar el siguiente comando en el terminal.

```
# rpm -qa | grep smbldap
```

la ejecucion del comando muestra la versión instalada y configurada de las herramientas de integración de Open Ldap y Samba.

```
smbldap-tools-0.9.6-3.el6.noarch
```

3.3 Instalación de un Controlador de Dominio Primario.

Para la validación de la instalación y configuración del SAMBA para el entorno de alta disponibilidad se utilizará el script de configuración llamado:

- Instalador_ldap_samba_p2.sh

```
clear
echo "            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "               DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "                INSTALACIÓN Y CONFIGURACIÓN SAMBA"
echo
"============================================================
==="
raiz="/OpenLdap_Samba_HA/configuraciones"
mv /etc/smbldap-tools/smbldap_bind.conf /etc/smbldap-tools/smbldap_bind.conf.bk
mv /etc/smbldap-tools/smbldap.conf /etc/smbldap-tools/smbldap.conf.bk
cp $raiz/smbldap_bind.conf /etc/smbldap-tools/smbldap_bind.conf
cp $raiz/smbldap.conf /etc/smbldap-tools/smbldap.conf
smbpasswd -w Jorge2013Armijo
echo "Creación de carpetas de profiles y netlogon"
```

Continuación del script de instalación y configuración de samba.

```
mkdir /home/netlogon && chmod 755 /home/netlogon
mkdir /home/profiles && chmod 777 /home/profiles
/etc/init.d/smb start
/etc/init.d/nmb start
groupadd -g 514 samba_domain_guests
groupadd -g 515 samba_domain_computers
groupadd -g 544 samba_administrator
groupadd -g 548 samba_account_operators
groupadd -g 550 samba_print_operators
groupadd -g 551 samba_backup_operators
groupadd -g 552 samba_replicators
chcon -R -t slapd_db_t /var/lib/ldap
authconfig --enableldap --enableldapauth --disablenis --enablecache --
ldapserver=127.0.0.1 --ldapbasedn=dc=jorge,dc=armijo,dc=com --updateall
/etc/init.d/smb restart
/etc/init.d/nmb restart
/etc/init.d/slapd restart
#cp $raiz/smbldap.conf /etc/smbldap-tools/smbldap.conf
smbldap-populate
/etc/init.d/smb restart
/etc/init.d/nmb restart
/etc/init.d/slapd restart
###################### desactivar el inicio de servicios para el cluster del OpenLdap +
Samba
/sbin/chkconfig slapd off
/sbin/chkconfig smb off
/sbin/chkconfig nmb off
###################### configurar smbldap-tools para cluster
mv /etc/smbldap-tools/smbldap.conf /etc/smbldap-tools/smbldap.conf.bk
cp $raiz/smbldap_cluster.conf /etc/smbldap-tools/smbldap.conf
```

Para la validación de la versión del Controlador de Dominio Primario Samba instalado en el sistema operativo se debe ejecutar el siguiente comando en el terminal.

```
# rpm -qa | grep samba
```

Esto listará todos los paquetes necesarios para la configuración de un controlador de dominio basado en samba.

```
samba-winbind-clients-3.6.9-151.el6.x86_64
samba-common-3.6.9-151.el6.x86_64
samba-winbind-3.6.9-151.el6.x86_64
samba-3.6.9-151.el6.x86_64
samba-client-3.6.9-151.el6.x86_64
```

3.4 Configuración de Archivos del LDAP.

Para la configuración del Protocolo Ligero de Acceso a Directorios (LDAP) se necesitan los siguientes archivos y sus configuraciones.

3.4.1 Configuración archivo principal para el LDAP.

El archivo principal de configuración es: /etc/openldap/slapd.conf.

De este archivo se puede destacar las siguientes líneas principales:

- Definición de la cabecera del directorio activo y el usuario con privilegios de administrador del directorio.

```
database        bdb
suffix          "dc=jorge,dc=armijo,dc=com"
checkpoint      1024 15
rootdn          "cn=Manager,dc=jorge,dc=armijo,dc=com"
```

- Índices de búsqueda de información del LDAP

```
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
index entryCSN                          eq
index entryUUID                         eq
index default                           sub
```

- Definición de permisos de lectura y escritura a grupos de usuarios del directorio.

```
access to *
        by
group/groupOfNames/member="cn=Administrators,ou=Group,dc=jorge,dc=armijo,dc=co
m" write
        by * break

access to *
        by self write
        by users read
        by anonymous read
        by * none
```

3.4.2 Configuración de certificados.

En el directorio /etc/openldap/cacerts contiene el certificado de autenticación que los equipos clientes Linux utilizarán para el acceso al directorio activo.

Este directorio contiene el archivo principal donde se muestra la llave pública de conexión la cual debe tener dos secciones, una donde describe a la llave de conexión y la otra donde está el certificado de autenticidad y debe ser similar a lo siguiente.

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC+
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
XIje7FuGAoDtKAWyTqNayFLFvxk8QYw81rXeK5+Bef4oSppm47c1
-----END CERTIFICATE-----
```

El certificado debe ser publicado en un sitio donde se pueda acceder por los clientes para poder hacer uso del mismo. Como puede ser en una dirección de un servidor ftp o apache para que los clientes Linux lo puedan descargar fácilmente.

3.5 Configuración de Archivos del SAMBA.

Para la configuración del Controlador de Dominio Principal se debe tener las siguientes alineaciones en el archivo principal. /etc/samba/smb.conf

3.5.1 Configuración archivo principal para el Samba

- Identificación del grupo de trabajo

```
workgroup = ORGANIZACION
netbios name = ORGANIZACION
securitv = user
```

- Sincronización de contraseñas OpenLdap y Samba

```
unix password sync = yes
ldap passwd sync = yes
passwd program = /usr/sbin/smbldap-passwd -u "%u"
```

- Definición de políticas de seguridad de usuarios

```
obey pam restrictions = yes
```

- Definición de Controlador de dominio.

```
domain logons = Yes
domain master = Yes
os level = 120
preferred master = Yes
wins support = Yes
```

- Definición de parámetros de conexión con OpenLdap.

```
passdb backend = ldapsam:ldap://192.168.12.20/
ldap admin dn = cn=Manager,dc=jorge,dc=armijo,dc=com
ldap suffix = dc=jorge,dc=armijo,dc=com
ldap group suffix = ou=Group
ldap user suffix = ou=People
```

- Definición de parámetros para la modificación de información del OpenLdap Samba a través de smbldap-tools.

```
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
```

Para la fácil creación, modificación, eliminación de directorios compartidos en el entorno de alta disponibilidad la realizaremos a través de la herramienta web grafica llamada Webmin.

Para instalarla ejecutaremos en el terminal:

```
yum install -y webmin
```

Para ingresar a la herramienta de administración en un navegador digitaremos:

```
https://192.168.12.20:10000
```

3.6 Ingreso de Información del Árbol.

Para el ingreso de información del directorio Activo se utilizará la herramienta de integración de OpenLdap + Samba el cual se basa en los esquemas definidos en el archivo /etc/opendladp/smbldap.conf

Esta información es llenada al ejecutar el script de instalación de samba a través de la ejecución del comando "smbldap-populate"

Al ejecutar el comando se definirá la estructura Base para el ingreso de información en el Directorio Activo, este comando genera contenido inicial sobre el cual se basará el directorio de la organización.

```
dn: dc=jorge,dc=armijo,dc=com
dc: jorge
objectClass: top
objectClass: domain

dn: ou=Hosts,dc=jorge,dc=armijo,dc=com
ou: Hosts
objectClass: top
objectClass: organizationalUnit

dn: ou=Rpc,dc=jorge,dc=armijo,dc=com
ou: Rpc
objectClass: top
objectClass: organizationalUnit

dn: nisMapName=netgroup.byuser,dc=jorge,dc=armijo,dc=com
nismapname: netgroup.byuser
objectClass: top
objectClass: nisMap

dn: ou=People,dc=jorge,dc=armijo,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=jorge,dc=armijo,dc=com
ou: Group
objectClass: top
objectClass: organizationalUnit

dn: ou=Netgroup,dc=jorge,dc=armijo,dc=com
ou: Netgroup
objectClass: top
objectClass: organizationalUnit
objectClass: organizationalUnit
```

3.7 Instalación y Configuración Herramientas Administración LDAP.

Para la validación de la instalación y configuración del de las herramientas de administración LDAP para el entorno de alta disponibilidad se utilizará el script de configuración llamado:

- instalador_phpldapadmin.sh

Para realizar la validación de la instalación y configuración de las herramientas de administración LDAP en el equipo se debe ejecutar el script llamado "instalador_phpldapadmin.sh" cuyo contenido es el siguiente:

```
#!/bin/sh
clear
echo "            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "               DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "            INSTALACIÓN Y CONFIGURACIÓN DE PHPLDAPADMIN"
echo "================================================="
raiz="/OpenLdap_Samba_HA/configuraciones"
#instalar phpldapadmin
yum install -y phpldapadmin httpd
#configuracion httpd NameServer
host=hostname
#configurar http-phpldapadmin
echo " ServerName $host " >> /etc/httpd/conf/httpd.conf
mv /etc/httpd/conf.d/phpldapadmin.conf /phpldapadmin.conf.old
cp $raiz/phpldapadmin.conf /etc/httpd/conf.d/phpldapadmin.conf
rm -rf /phpldapadmin.conf.old
# configurar php para el phpldapadmin
mv /usr/share/phpldapadmin/config/config.php /config.php
cp $raiz/config.php /usr/share/phpldapadmin/config/config.php
rm -rf /config.php
/etc/init.d/httpd start
/sbin/chkconfig httpd on
```

3.7.1 Configuración Smbldap-tools.

Para la configuración de smbldap-tools se debe hacer uso de un repositorio externo de software el llamado epel del proyecto comunitario de fedora que ya se encuentra configurado en el repositorio local creado.

Los archivos de configuración son:

- En el archivo /etc/smbldap-tools/smbldap_bind.conf en el cual de definirá las credenciales para la validación de los servicios principal y secundario para el OpenLdap y Samba.

```
slaveDN="cn=Manager,dc=jorge,dc=armijo,dc=com"
slavePw="Jorge2013Armijo"
masterDN="cn=Manager,dc=jorge,dc=armijo,dc=com"
masterPw="Jorge2013Armijo"
```

- En el archivo /etc/smbldap-tools/smbldap.conf definiremos los parámetros de configuración entre OpenLdap y Samba.
- Entre los parámetros de configuración los más importantes están:
  - SID="S-1-5-21-2323392562-1448967901-2013120882" con el cual se identifica cada uno de los miembros del directorio.
  - sambaDomain="ORGANIZACION" con el cual se identifican los equipos Windows
  - slaveLDAP="127.0.0.1" define la url del servidor secundarios de OpenLdap
  - masterLDAP="192.168.12.20" define la url del servidor secundarios de OpenLdap
  - Para validar lo manifestado de debe ejecutar en el terminal el comando:

```
# net getlocalsid
```

Esto nos devolverá el SID definido para el Domino “Organizacion”

```
SID for domain ORGANIZACION is: S-1-5-21-2323392562-1448967901-2013120882
```

Para validar la configuración de consulta de información ejecutamos en el terminal:

```
ldapsearch -x -h 192.168.12.20 | grep jarmijo
memberUid: jarmijo
memberUid: jarmijo
memberUid: jarmijo
memberUid: jarmijo
# jarmijo, Agencia Norte, People, jorge.armijo.com
dn: uid=jarmijo,ou=Agencia Norte,ou=People,dc=jorge,dc=armijo,dc=com
uid: jarmijo
homeDirectory: /home/jarmijo
sambaHomePath: /home/jarmijo
```

3.7.2 Instalación y configuración Phpldapadmin.

Para la instalación y configuración de Phpldapadmin se debe hacer uso de un repositorio externo de software el llamado epel del proyecto comunitario de fedora.

Para el caso de esta guía ya se configuro el repositorio de epel y cuenta con los paquetes necesarios para la instalación y configuración del Phpldapadmin los cuales son:

```
lighttpd-1.4.32-1.el6.x86_64.rpm
perl-Crypt-SmbHash-0.12-10.el6.noarch.rpm
perl-Digest-MD4-1.5-1.2.el6.rf.x86_64.rpm
perl-Jcode-2.07-1.el6.noarch.rpm
perl-Unicode-Map-0.112-1.el6.rf.x86_64.rpm
perl-Unicode-Map8-0.13-1.el6.rfx.x86_64.rpm
perl-Unicode-MapUTF8-1.11-10.el6.noarch.rpm
perl-Unicode-String-2.09-12.el6.x86_64.rpm
phpldapadmin-1.2.3-1.el6.noarch.rpm
```

Para realizar la instalación ejecutar en un terminal:

```
# yum install phpldapadmin
```

Para realizar una configuración con los campos requeridos editaremos el archivo /usr/share/phpldapadmin/config/config.php sobre el cual está la configuración de la herramienta y modificaremos las líneas:

```
$servers->setValue('server','name','Cluster LDAP Server Jorge Armijo');
$servers->setValue('server','host','192.168.12.20');
```

Las cuales nos permitirán acceder a la IP configurada para el clúster del OpenLdap-Samba

3.8 Instalación de un Sistema de Alta Disponibilidad.

Para la instalación y configuración de un entorno de Alta disponibilidad sobre Red Hat se debe habilitar dos grupos de repositorios especiales el de “HighAvailability” y el de “ResilientStorage”.

El entorno de alta disponibilidad en Red Hat que se conoce como Conga el cual tiene los componentes “luci” que es la consola de administración y “ricci” que viene a ser el agente de monitoreo de servicios en los nodos que conforman el entorno de alta disponibilidad.

Para la validación de la instalación y configuración del de las herramientas para el entorno de alta disponibilidad se utilizara el script de configuración llamado:

- instalador_HA.sh

Para realizar la validación de la instalación y configuración de las herramientas de administración LDAP en el equipo se ejecutará el script llamado “instalador_HA.sh” cuyo contenido es el siguiente:

```
#!/bin/sh
clear
echo "            PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR"
echo "               DISERTACIÓN DE GRADO JORGE ARMIJO"
echo "          INSTALACIÓN Y CONFIGURACIÓN DEL ENTORNO DE ALTA DISPONIBILIDAD"
echo
"============================================================="
raiz="/OpenLdap_Samba_HA/configuraciones"
#instalar entorno de alta disponibilidad
echo "Instalación paquetes para el fencing"
yum install -y fence-virt fence-virtd fence-virtd-libvirt fence-virtd-multicast fence-virtd-serial fence-agents fence-virtd-checkpoint fence-virtd-multicast fence-virtd-serial
/sbin/chkconfig fence_virtd on
/sbinchkconfig libvirtd on
/sbin/chkconfig libvirt-guests on
clear
echo "Instalación de Grupos de paquetes para Entorno de alta disponibilidad"
yum groupinstall -y "High Availability"
yum groupinstall -y "Resilient Storage"
chkconfig ricci on
chkconfig cman on
chkconfig rgmanager on
chkconfig modclusterd on
chkconfig clvmd on
clear
echo "Configuración del contraseña del agente de alta disponibilidad ricci"
/usr/bin/passwd ricci
echo "Recordar la contraseña para la posterior configuración del nodo en la consola de Administración del Cluster"
mv /etc/sysconfig/selinux /etc/sysconfig/selinux.bk
cp $raiz/selinux /etc/sysconfig/selinux
echo "El servidor sera reiniciado para finalizar la configuracion"
reboot
```

Los paquetes que componen el grupo de “Resilent Storage” son:

```
yum list installed | grep "@ResilientStorage"
gfs2-utils.x86_64              3.0.12.1-49.el6        @ResilientStorage
lvm2-cluster.x86_64            2.02.98-9.el6          @ResilientStorage
```

Los paquetes que componen el grupo de “HighAvailability”son:

```
yum list installed | grep "@HighAvailability"
ccs.x86_64                     0.16.2-63.el6          @HighAvailability
cluster-glue-libs.x86_64       1.0.5-6.el6            @HighAvailability
clusterlib.x86_64              3.0.12.1-49.el6        @HighAvailability
cman.x86_64                    3.0.12.1-49.el6        @HighAvailability
corosync.x86_64                1.4.1-15.el6           @HighAvailability
corosynclib.x86_64             1.4.1-15.el6           @HighAvailability
fence-virt.x86_64              0.2.3-13.el6           @HighAvailability
fence-virtd-checkpoint.x86_64  0.2.3-13.el6           @HighAvailability
modcluster.x86_64              0.16.2-20.el6          @HighAvailability
omping.x86_64                  0.0.4-1.el6            @HighAvailability
openais.x86_64                 1.1.1-7.el6            @HighAvailability
openaislib.x86_64              1.1.1-7.el6            @HighAvailability
resource-agents.x86_64         3.9.2-21.el6           @HighAvailability
rgmanager.x86_64               3.0.12.1-17.el6        @HighAvailability
ricci.x86_64                   0.16.2-63.el6          @HighAvailability
```

3.8.1 Instalación y configuración de la consola de administración

Para la instalación y configuración de la consola de administración ejecutamos el script de instalación y configuración “instalación_HA.sh”. Este script instala los paquetes necesarios para la configuración que un nodo del clúster necesita para ser miembro del mismo.

Para que un equipo tenga el comportamiento que del administrador del entorno de alta disponibilidad hay que instalar un paquete adicional llamado “luci”.

```
# yum install luci
```

Este paquete instalara la consola de administración Web y componentes para mantener la comunicación entre este equipo y los demás nodos que conforman el entorno de alta disponibilidad de OpenLdap-Samba.

Para la versión que se utilizará en esta guía no es necesario crear un usuario por línea de comandos para ingresar a la herramienta de administración como era necesario en versiones anteriores.

Para el ingreso a la herramienta de administración se realizará con el usuario “root”, y su contraseña del sistema, posteriormente se configurara el o los usuarios que acceden a la herramienta y los permisos respectivos.

3.8.2 Instalación y configuración de los nodos del clúster.

Para la instalación y configuración de los nodos del entorno de alta disponibilidad ejecutar en el terminal. El script de “instalador_HA.sh” en el cual se realiza la instalación de los paquetes de alta disponibilidad y de almacenamiento compartido.

En el grupo llamado alta disponibilidad se instalan todas las herramientas necesarias para habilitar la alta disponibilidad en un equipo configurado como nodo. Además de este grupo de paquetes debemos instalar los paquetes para la administración del almacenamiento compartido que están disponibles en el grupo de paquetes llamado Resilent Storage

La configuración del entorno de alta disponibilidad se lo realizará directamente desde la herramienta de administración web.

Esta configuración es almacenada en el directorio /etc/cluster/cluster.conf la cual dispone de dos secciones que se describen a continuación:

En la primera definimos los miembros del clúster y debe ser similar a lo siguiente.

```
<cluster config_version="32" name="OpenLdap-Samba">
    <clusternodes>
        <clusternode name="clster1.jorgearmijo.com" nodeid="1">
            <fence>
                <method name="fence-nodo1">
                    <device domain="clster-nodo1" name="kvm"/>
                </method>
            </fence>
        </clusternode>
        <clusternode name="clster2.jorgearmijo.com" nodeid="2">
            <fence>
                <method name="fence-nodo2">
                    <device domain="clster-nodo2" name="kvm"/>
                </method>
            </fence>
        </clusternode>
        <clusternode name="clster3.jorgearmijo.com" nodeid="3">
            <fence>
                <method name="fence-nodo3">
                    <device domain="clster-nodo3" name="kvm"/>
                </method>
            </fence>
        </clusternode>
    </clusternodes>
```

En la segunda sección del archivo /etc/cluster/cluster.conf definimos los servicios que serán parte del clúster.

```
    <fencedevices>
        <fencedevice agent="fence_xvm" name="kvm"/>
     </fencedevices>
     <rm>
        <failoverdomains>
            <failoverdomain name="Dominio-OpenLdap-Samba" ordered="1">
                <failoverdomainnode name="clster1.jorgearmijo.com" priority="1"/>
                <failoverdomainnode name="clster2.jorgearmijo.com" priority="2"/>
                <failoverdomainnode name="clster3.jorgearmijo.com" priority="3"/>
            </failoverdomain>
        </failoverdomains>
        <resources>
            <ip address="192.168.12.20/16" sleeptime="15"/>
            <openldap config_file="/etc/openldap/slapd.conf" name="srv-clster-OpenLdap"
shutdown_wait="0" url_list="ldap://192.168.12.20/"/>
            <samba config_file="/etc/samba/smb.conf" name="srv-clster-Samba"
shutdown_wait="0"/>
            <clusterfs device="/dev/openldap/varlibldap" force_unmount="1" fsid="29080"
fstype="gfs2" mountpoint="/var/lib/ldap" name="gfs-openldap" options="rw" self_fence="1"/>
            <clusterfs device="/dev/samba/samba-data" force_unmount="1" fsid="34624"
fstype="gfs2" mountpoint="/samba-archivos" name="gfs-samba" options="rw" self_fence="1"/>
        </resources>
        <service domain="Dominio-OpenLdap-Samba" name="Grp_srv-OpenLdap-Samba"
recovery="relocate">
            <ip ref="192.168.12.20/16"/>
            <openldap ref="srv-clster-OpenLdap">
                <clusterfs ref="gfs-openldap"/>
            </openldap>
            <samba ref="srv-clster-Samba">
                <clusterfs ref="gfs-samba"/>
            </samba>
        </service>
    </rm>
```

En la cual se define la dirección Ip que se utilizará para el acceso de los servicios y el detalle de los servicios configurados en el Cluster.

Para validar cuantos miembros del clúster están activos ejecutar en un terminal:

```
# clustat
```

Esto nos indica que hay un clúster con el nombre de OpenLdap-Sama y que tiene 3 miembros activos y que en el servidor con el hostname clster1.jorgearmijo.com está ejecutándose los servicios de OpenLdap y Samba además de tener configurada una dirección Ip Flotante para el acceso al clúster.

```
Cluster Status for OpenLdap-Samba @ Tue Nov 19 14:56:36 2013
Member Status: Quorate

 Member Name                                              ID   Status
 ------ ----                                              ---- ------
 clster1.jorgearmijo.com                                  1 Online, Local, rgmanager
 clster2.jorgearmijo.com                                  2 Online, rgmanager
 clster3.jorgearmijo.com                                  3 Online, rgmanager

 Service Name                         Owner (Last)                   State
 ------- ----                         ----- ------                   -----
 service:Grp_srv-OpenLdap-Samb        clster1.jorgearmijo.com        started
```

CAPITULO 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones.

El presente trabajo de disertación de grado tuvo como objetivo principal el desarrollo de una guía metodología para la Implementación de un Protocolo Ligero de Acceso a Directorios con un Controlador de Dominio Principal en un entorno de alta disponibilidad sobre una plataforma Linux, en la cual demostramos como se debe realizar la configuración y validación del funcionamiento de cada uno de los componentes de esta guía.

4.1.1 Las funcionalidades prestadas por un Protocolo Ligero de Acceso a Directorios y combinadas con las del Controlador de Domino Principal en un entorno de alta disponibilidad nos permiten brindar entornos de red en los cuales pueden coexistir sistemas operativos libres y privativos bajo plataformas Linux y Windows. Además de mantener la disponibilidad del servicio en el esquema de 24 horas x 7 días.

4.1.2 Las configuraciones del Protocolo Ligero de Acceso a Directorios permite definir un esquema organizacional de acuerdo a las estructuras jerárquicas de cada organización, lo que facilita establecer niveles en la administración y control la estructura del mismo.

4.1.3 Otro aspecto importante que se puede destacar de la configuración del Protocolo Ligero de Acceso a Directorios es que permite realizar la configuración de varios servidores principales como estrategia para obtener el respaldo de toda la información como plan de contingencia ante cualquier siniestro que pueda suscitarse.

4.1.4 Las configuraciones del Controlador de Dominio Principal permiten establecer medios de comunicación entre varias plataformas de Sistemas Operativos así por ejemplo, permite mantener el control y el acceso a los recursos de red con equipos bajo plataformas Linux y Windows centralizados en una sola herramienta de administración.

4.1.5 Otra de las ventajas que brindan las configuraciones de un entorno de alta

disponibilidad es que permiten realizar mantenimientos en la infraestructura de los servidores que conforman el clúster, sin tener que interrumpir su normal y correcto funcionamiento reduciendo así al máximo el tiempo de inoperatividad del servicio en un tiempo definido.

4.1.6 El desarrollo de esta guía metodológica ha permitido establecer parámetros para la instalación y configuración de los servicios de OpenLdap, Samba en un entorno de alta disponibilidad de forma fácil y ágil a través de scripts con varias configuraciones preestablecidas, las cuales facilitarán la implementación del mismo en entornos pequeños medianos o grandes dependiendo de los requerimientos de cada organización.

4.2 Recomendaciones.

Las recomendaciones generadas luego del desarrollo de la guía metodológica para la Implementación de un Protocolo Ligero de Acceso a Directorios con un Controlador de Dominio Principal en un entorno de alta disponibilidad sobre una plataforma Linux son las siguientes:

4.2.1 Se recomienda hacer un levantamiento de información previo a la implementación sobre el cual estará basado el Protocolo Ligero de Acceso a Directorios. Esto facilitará el definir los esquemas que serán configurados en el OpenLdap y Samba y la información que este contendrá.

4.2.2 Se recomienda realizar un análisis del organigrama de la empresa previo a la definición estructural del Protocolo Ligero de Acceso a Directorios. Esto nos permitirá modificar los scripts de instalación y configuración del entorno de alta disponibilidad de OpenLdap y Samba de acuerdo a las necesidades de cada empresa. De esta manera garantizamos la satisfacción del cliente y optimizamos al máximo el tiempo de trabajo y reduciendo el tiempo de implementación.

4.2.3 Se recomienda definir un mapa de la topología de la red sobre la cual se implementara el entorno de alta disponibilidad de OpenLdap y Samba. Esto nos permitirá mantener clara una idea de los servidores que formaran parte del clúster.

4.2.4 Se recomienda aplicar esta configuración cuando se disponga de número de personal y

que dependa su trabajo de este servicio y sobre todo cuando este sea utilizado en más de una locación física, de esta forma al mantener un esquema de alta disponibilidad de OpenLdap y Samba se puede brindar un servicio de 24horas y 7dias a la semana sin presentar interrupciones por mantenimientos a los equipos o a las configuraciones del servicio.

4.2.5 Se recomienda que para la implementación de esta solución la infraestructura disponga mínimo de tres equipos dos de los cuales serán destinados a ser los nodos con los servicios, el tercero debe ser destinado para la implementación de la consola de administración de los nodos.

4.2.6 Se recomienda que los servidores dispongan mínimo de 250Gb de disco local para el funcionamiento del sistema operativo y servicios, al menos 8Gb de RAM y un Dispositivo de almacenamiento compartido para el uso del Directorio Activo.